Introduction

As the global economy continues to further embrace digital transformation, IT has become essential to almost every facet of the modern business. Yet while the advances and increasing adoption of digital technologies have had a profound, positive impact when delivering on strategic priorities, one thing remains true. The event of an IT outage — total or partial — has massive implications to a business’s continuity. In fact, 66% of enterprises admit that their digital transformation initiatives are being held back by unplanned downtime.

Threats to IT service and business continuity come in all shapes and sizes. Planned and unplanned. Accidental or intentional. Man-made or natural. Regardless of the reason for outage, it is imperative to plan for disaster recovery (DR), whether that disaster results in the outage of a single service or application, or the entire IT infrastructure.
Disaster recovery challenges

Planning for DR is not a new strategy — it’s been around for decades. However, the problem with a decades-old approach is that it isn’t designed for today’s abundance of and reliance on IT infrastructure. Forrester reports that just 18% of surveyed businesses feel very prepared to recover their data center in the event of a site failure or disaster. Legacy solutions just cannot cope with a constantly changing, ever-complex IT environment. There’s more to protect and manage, with strict service-level objectives (SLOs) and near-zero tolerance for downtime. Expensive, manual processes are neither scalable, efficient nor cost-effective. A modern DR solution must be as fast and efficient as the applications, services and infrastructure that it’s designed to protect.

DR also has compliance implications — laws, regulations and standards set in place to ensure an organization’s responsibility to the reliability, integrity and Availability of its data. Compliance varies from industry to industry, but one thing holds true — compliance deficiencies are not an option, with significant financial and reputational risks.

This begs the question, if many businesses have DR plans in place, why do the majority feel that their Availability — and compliance — are at risk? We can break this down into four critical components; the plan itself, documenting the plan, testing the plan and the actual execution of failover and failback.
At the heart of every successful DR plan is knowing what to protect and how to protect it. Analyses and assessments are critical when it comes to determining which elements of the IT infrastructure are essential to business operations. Understand and define the outage risks and their impact, tolerance for downtime and the processes and procedures necessary to restore access.

*What are the mission-critical and business-critical services and applications?*

*What are the operational and financial consequences of losing access to such services?*

*How often must we be able to recover to a point in time?*

*How quickly must we be able to recover to meet the needs of the business?*

*How often do we need to reevaluate?*

Documenting the DR plan is critical to any successful DR strategy. Documentation clearly defines the DR plan in its entirety and most importantly, the established processes and procedures to follow in the event of an outage. Manually documenting the DR plan can be an expensive and lengthy process, especially for larger environments and the continual changes occurring.

This is evidenced with only 14% or organizations updating their DR plans and documentation continually². Outdated and improper DR documentation doesn’t just put the business’s Availability at risk though.

Audits are common and may identify failure when complying with regulatory and legal standards, with the inability to prove security, resiliency and recoverability resulting in expensive fines and reputational damage.
Testing is a critical component when it comes to ensuring preparedness, yet only 19% of surveyed organizations run a full test more than once per year. An unacceptable frequency when considering the reliance on a constantly changing IT environment. Frequent end-to-end testing can prove challenging, especially when we consider the preparation and resources required to conduct a full test of all systems and their dependencies, without impacting the production environment and interrupting end users.

The constant state of change within ever-complex IT environments are a key point of failure when performing failover. Mismatches resulting from uncaptured changes to systems or configurations are the most common technology impediments to a successful recovery, particularly when we consider the dependencies one application or service may have on another. As one IT service is impacted by an IT outage, it causes a chain reaction and affects the performance and/or Availability of others, cascading those failures into even more systems. Manually powering these on in perfect sequence is next to impossible, especially when we may be dealing with hundreds, maybe thousands of services, severely impacting what can be recovered, and how long it takes.
Veeam Availability Orchestrator

To solve these common challenges faced by businesses of all sizes and industries, Veeam® has developed Veeam Availability Orchestrator.

A highly-automated and resilient orchestration engine designed specifically to help organizations satisfy compliance requirements, minimize downtime and ensure the continuous delivery of production IT services.

Reduce the time, cost and effort associated with planning for and recovering from a disaster through the automatic creation, documentation and testing of DR plans, fully prepared for C-level executive and stakeholder signoff, proving compliance with industry regulations and audits.
Veeam Availability Orchestrator automatically creates and delivers regular, in-depth documentation on a scheduled and on-demand basis, enabling you to meet your DR plan documentation needs for legal requirements, compliance audits and your technical libraries. The fully customizable, template-based DR documentation is available in four plan report types: A definition report, readiness check report, test execution report and execution report.

Definition reports contain the configuration of the DR plan and its components, automatically updated and republished daily as the virtual environment changes, detailing and communicating what was changed, when it was changed and by whom.

The plan readiness check report sanity-checks and documents the readiness of the DR plan, by comparing plan configuration with the status of the DR environment — with no need to start any VM replicas. This makes it incredibly efficient with zero impact. Readiness check reports are automatically updated daily, and are also available on-demand.

Execution and test execution reports are generated upon the completion of a real-world and/or test failover or failback. The information contained within these reports is ideal for evaluating and troubleshooting, as well as identifying areas of the DR plan that can be improved upon to better the efficiency, effectiveness and speed of failovers.

With detailed documentation of components, configurations, processes and procedures, end-to-end reliability in the event of an outage is ensured. This detailed, up-to-date documentation also ensures compliance through the demonstration of the security and recoverability of critical data.
Automated testing

Veeam Availability Orchestrator delivers comprehensive testing and readiness checks of a business’s DR plan on a scheduled or on demand basis, without impact to production systems.

Testing of the DR plan is performed within enhanced Veeam virtual labs, an isolated virtual environment where VMs can be verified without the extra provisioning of resources. The virtual lab mirrors the production environment’s network configuration, allowing for real world testing to take place just as if it were in the production environment. And, as it is fully fenced off from the production environment, regular testing of the DR plan — either scheduled or on demand — can occur without any impact to production systems or end users.

Testing is fully automated, avoiding expensive and time-consuming manual processes. This ease-of-use, combined with the zero-impact nature makes frequent testing achievable, no matter the size of environment.

The plan’s reliability and readiness is delivered in the previously mentioned documentation, as well as real-time reports and dashboards, ensuring that all mission and business-critical VMs, applications and services are recoverable and error-free.
A DR plan is only as good as its ability to reliably execute failover (and eventually failback) in its time of need. Veeam Availability Orchestrator ensures IT service continuity and minimizes service disruption through automated, reliable failover and failback of single or multi-site plans for DR. This too can apply to disaster avoidance and planned migrations.

Access to DR resources is regulated through role-based access control (RBAC), ensuring that only those with authorization have access to DR plans, as well as the ability to execute failovers. This also ensures there is no human single-point-of-failure should the need to failover occur.

VM, service and application startup sequences are predefined within the plan for successful, automated execution of a failover or failback. A faster, more successful recovery is ensured as critical servers — such as the database servers — are powered on before the other VMs, services and applications that have dependencies on them.

Before Veeam Availability Orchestrator performs the correct sequential startup of all VMs, services and applications, verification checks are also performed. Verification of VMs includes network and heartbeat checks to ensure it is running, before moving on to the next.

Optional application verifications (such as database, mail and web) are also available through predefined scripts, with the ability to add and run custom scripts, too.

Triggering failover and failback is achieved through the Veeam Availability Orchestrator user interface (UI). Failover and failback execution can also be performed within other enterprise applications thanks to Veeam Availability Orchestrator’s RESTful API, consolidating your business continuity workflows into a single tool.
Conclusion

It’s clear that legacy approaches to DR planning and strategies are not equipped to deal with digital transformation initiatives and the evolving data center, hindering adoption and growth of new technologies and the business.

Solutions that enable orchestration and automation of DR and compliance are leading the way to greater business continuity, helping to ensure the continuous delivery of production IT services that businesses rely on and compliance with industry regulations.

Veeam Availability Orchestrator allows businesses of all sizes to achieve these higher levels of resiliency and Availability through its ability to dynamically document, automatically test and reliably execute DR plans, reducing the time, costs and effort associated when planning for and recovering from a disaster.

References
1. ESG Availability Report, 2017
2. Forrester, The State of Business Technology Resiliency, Q2 2017