Designed by biomni

JobR

Why Backup Service Assurance is integral to a modern enterprise IT infrastructure

We investigate the challenges that businesses are facing with their Backup Service Assurance processes and systems. We look into what can be done to resolve these issues through a SaaS-based solution.

STARTING READING

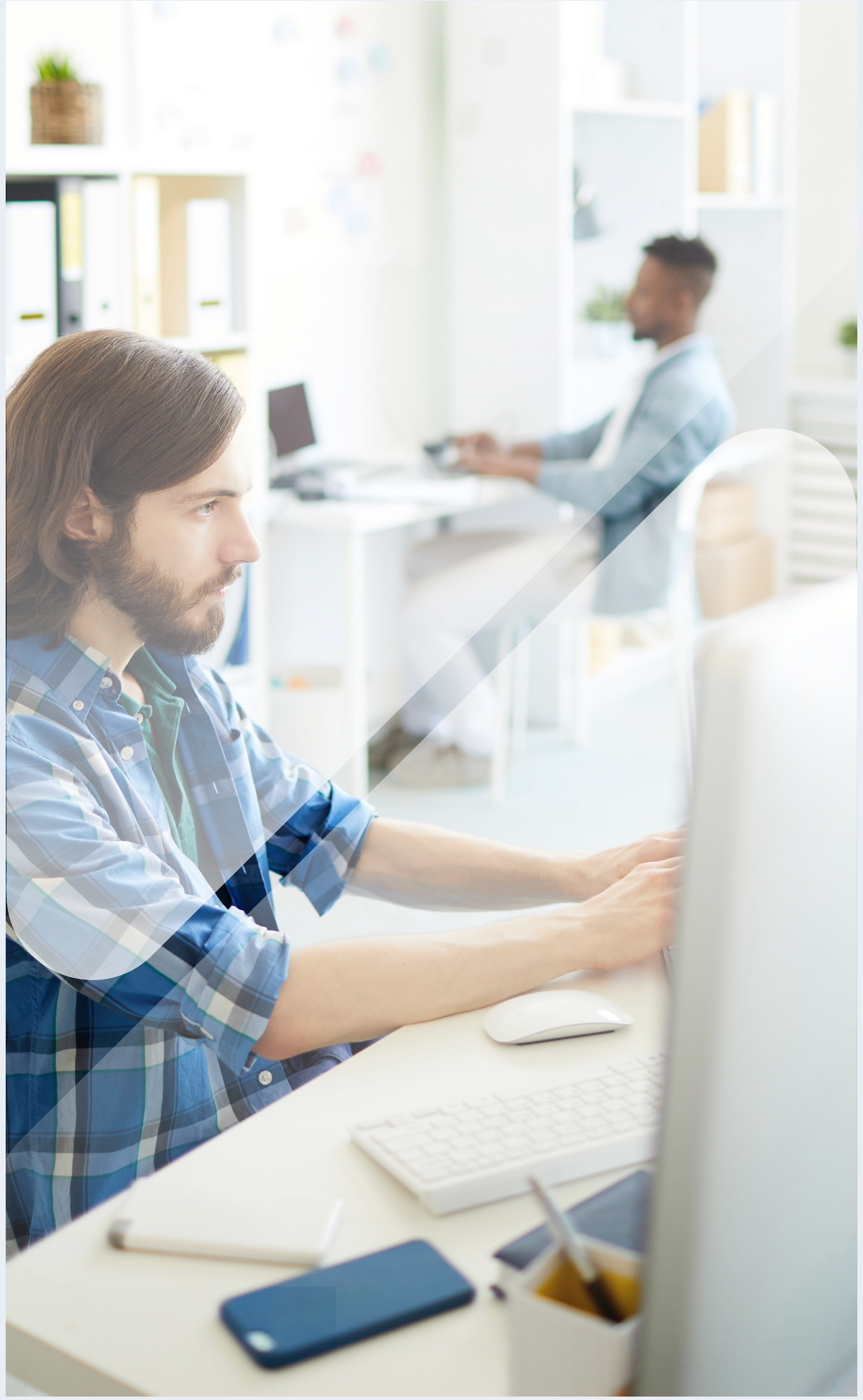
What is a Backup Service Assurance?

Backup Service Assurance refers to the process and systems put in place to ensure the reliability, integrity, and availability of backup services in an IT environment. It encompasses various activities aimed at **guaranteeing that data backups are performed successfully** and can be restored when needed, all to help meet **SLA** and **compliance standards**.

The goal of Backup Service Assurance is to **minimise the risks associated with data loss** or unavailability during adverse events such as cyberattacks, hardware failures, software glitches, or human errors.

It involves implementing strategies, tools, and practices to enhance the overall reliability and effectiveness of backup processes.

By implementing robust Backup Service Assurance measures, organisations can mitigate the risks associated with data loss, minimise downtime, ensure compliance, and maintain business continuity. It provides confidence that critical data can be recovered reliably and efficiently when needed, safeguarding the organisation's operations, reputation, and customer trust.



Challenges Customers face in their Backup Service

Challenge 1

The ability to **recover data swiftly during adverse events** is crucial for maintaining business continuity. Whether dealing with cyber threats, failures in IT components, or human errors, the successful recovery of data is paramount. However, **managing backups becomes increasingly complex** when organisations implement multiple backup domains, use different vendors' backup solutions, or offer different tiers of backup services.

Challenge 2

The integrity of backup processes, which involves detecting failures, diagnosing their root causes, and prioritising remediation, is **more challenging with diverse data sources that backup teams handle daily**. Additionally, heightened business and **regulatory scrutiny** means backup teams must provide evidence that demonstrates compliance with internal and external policies and regulations related to business and cyber risks.

Challenge 3

If your business offers Backup-as-a-Service as part of a Managed Services, then it is essential to **deliver insights** so your customers can monitor your service's performance against SLAs and compliance mandates. Unfortunately, native backup management solutions **often fall short** in meeting these requirements, burdening backup teams and **diverting expert resources away** from productive operational activities.

"With the average reported time to recover from a cyberattack in the second quarter of 2022 being **24 days** — a devastating amount of downtime for mission-critical systems — addressing these challenges has never been more critical."

Gartner® Research *"How to Build a Secure Environment to Recover From Ransomware and Other Cyberattacks"*, Fintan Quinn, April 2023

The need for change in the way we backup

Failure to meet these issues has many detrimental business impacts

- **Failure to recover data from backups** has material impact on company revenue, share price and can even completely stop businesses from functioning.
- **Increases insurance premiums** associated with cyber and business risks.
- An inability to make **successful insurance claims** in events where data cannot be recovered.
- An inability to **demonstrate compliance with policies and regulations** could have a detrimental impact on their ability to compete and even conduct business in markets where they are present.
- Failure to meet or demonstrate a business is **meeting SLAs and compliance objectives** may result in financial penalties and lost contracts.

We've seen how functioning Backup systems and services are paramount to a business's success and that current solutions on the market are complicated and require significant IT resource in human resources and capital investment.

> The consistency and speed that proper automation adds is arguably what elevates a backup system to a **data resilience strategy**. You can trigger restores based on monitoring or observability events and architect the backup and restore of complex applications that require consistent state across multiple pieces of infrastructure or even disparate platforms.

Forrester Research *"Top Seven Components Of Data Resilience In A Multicloud World"*,
Brent Ellis, July 2022

strategy

Key components of Backup Service Assurance include:

Backup Monitoring

Continuous monitoring of backup systems and processes to detect failures, errors, or anomalies. This ensures prompt identification of any issues that may impact backups.

Backup Testing and Validation

Regular testing and validation of backup data to ensure its integrity to verify it can be restored. This involves performing restoration drills and verifying the recoverability of critical data.

Incident Management

Establishing processes and procedures to handle backup-related incidents helping resolve issues promptly and prevent future incidents.

Compliance and Reporting

Ensuring that backup processes comply with internal and external policies, regulations, and industry standards.

Automation and Orchestration

Utilising automation and orchestration tools to streamline and optimise backup operations.

Performance Monitoring and Optimisation

Monitoring the performance of backup systems to make necessary adjustments that optimise efficiency. This involves analysing backup metrics, identifying bottlenecks, and implementing improvements to enhance backup speed and reliability.

JobR Backup Service Assurance

Backup Service Assurance solution, JobR has been purpose-built to address these challenges. JobR is a **Software-as-a-Service** (SaaS) platform designed specifically to grant businesses backup service assurance with the following capabilities:

1. Unified View

JobR provides a single pane of glass that **consolidates information from multi-domain and multi-vendor backup environments**. This eliminates the need for backup teams to navigate through multiple consoles to detect and address backup failures.

2. Actionable Insights

JobR's analytics **provide meaningful insights**, including business context, ensuring that backup failures are promptly identified and prioritised based on their impact on business criticality. This enables backup administrators to focus their efforts on resolving the most critical issues first.

3. Integration with Incident and Change Management Tools

JobR integrates with third-party tools used for incident and change management. This allows backup teams to have a comprehensive view of adverse events that cause backup failures, even if those events are outside their control.

JobR Backup Service Assurance

4. Expert Knowledge Base

JobR incorporates a knowledge base that includes historical failure data, remedial actions, and vendor expertise. This **empowers first and second-line support teams** to play a more prominent role in the backup service assurance process, leveraging prior knowledge to resolve issues effectively.

5. Workflow/Orchestration Capabilities

JobR offers workflow and orchestration capabilities, enabling the automated detection, diagnosis, and remediation of common backup failures. This automation **frees up experts' time**, allowing them to focus on other critical tasks, while eliminating the need for developing and maintaining custom scripts and automation.

6. Reporting Capabilities

JobR provides **out-of-the-box and customisable** reporting capabilities, eliminating the need for in-house development of bespoke reporting solutions.

Centralised management and reporting helps IT professionals **manage global, heterogeneous infrastructure** with ease and also gives decision-makers and risk management professionals a **top-down look** at the overall **resilience** posture of the organisation.

Forrester Research *“Top Seven Components Of Data Resilience In A Multicloud World”*,
Brent Ellis, July 2022

Conclusion

Designed by biomni

JobR

By leveraging the capabilities of JobR, organisations can achieve several benefits to realise their return on investment including:

- **Drastically reduce the risk of data recovery failure** in the face of cyber attacks, IT failures, and human errors.
- **Streamline backup service assurance processes** and reduce operational costs by enabling non-specialists to handle more tasks.
- **Meet reporting obligations** mandated by internal and external stakeholders.
- **Eliminate the need for development work**, such as scripts, automation, and custom reports, to support backup service assurance processes.
- **Reduce insurance premiums** associated with cyber and business risks.
- **Avoid financial losses** resulting from SLA breaches and cyber events.

In summary, a backup automation system like JobR simplifies the management of backup processes, ensures data recovery success, and supports compliance with policies and regulations. It empowers backup teams to focus on critical tasks while delivering cost savings and mitigating risks associated with cyber threats and operational failures.

SEE MORE

Designed by biomni

JobR

TRY JOBR TODAY

Speak to us and discover Backup Service Assurance for your organisation with a free trial or demonstration of JobR today

Let’s talk

VISIT

biomni.com/jobr

MSP OR PARTNER?

Uncover new opportunities in an overlooked gap in the backup space

Start selling Backup Assurance today

Discover more