keepit®

Evaluating SaaS backup and recovery vendors

A complete checklist of questions to guide your selection

Table of contents

INTRODUCTION

RFI QUESTIONS EXPLAINED

IN SUMMARY

Introduction

In today's digital-first world, organizations can't afford downtime. Achieving true resilience means treating disaster recovery (DR) and business continuity management (BCM) as core business functions, not just IT responsibilities. At Keepit, we've created a disaster recovery maturity framework specifically for SaaS applications to help organizations benchmark their own SaaS DR capabilities and to highlight areas for improvement.

The framework introduces five distinct stages of maturity and provides strategic recommendations on how to advance to the next level of preparedness. Organizations at the "managed" stage stand out: They execute complex recoveries confidently, integrate DR with security, communications, and compliance processes, and maintain clear observability across systems to detect issues before they become problems.

Senior leadership owns and budgets for DR and BC (business continuity), ensuring recovery plans are robust and aligned with the business' needs for regulation and compliance.

This request for information (RFI) checklist is designed to help organizations identify vendors that can support them in achieving "managed" status. By responding to these questions, vendors demonstrate how they enable mature DR practices, giving organizations clear insight into which partners can help close gaps and strengthen overall resilience.

Scoring system

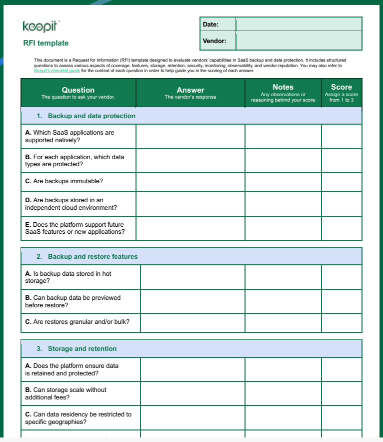
This RFI checklist is designed to help you evaluate SaaS backup and data protection vendors consistently. For each question, we suggest scoring answers on a 1–3 scale, where 3 indicates the most comprehensive solution, 2 indicates adequate coverage, and 1 indicates limited or no support. Using the same scale for all questions helps you quickly identify which vendors offer the strongest capabilities overall. A top score reflects capabilities consistent with what we define as "managed" organizations in the DR maturity framework, where predictive monitoring, anomaly detection, and integrated reporting enable proactive resilience.

Want the full template?

Download it here.

Prefer the deeper dive? Keep reading for a breakdown of every question — and why it matters. Use these explanations to guide conversations internally and ensure consistent, objective assessments.

Download now



keepit

RFI template

Date:	
Vendor:	

This document is a Request for Information (RFI) template designed to evaluate vendors' capabilities in SaaS backup and data protection. It includes structured questions to assess various aspects of coverage, features, storage, retention, security, monitoring, observability, and vendor reputation. You may also refer to Keepit's checklist guide for the context of each question in order to help guide you in the scoring of each answer.

Question The question to ask your vendor.	Answer The vendor's response	Notes Any observations or reasoning behind your score	Score Assign a score from 1 to 3
1. Backup and data protection			
A. Which SaaS applications are supported natively?			
B. For each application, which data types are protected?			
C. Are backups immutable?			
D. Are backups stored in an independent cloud environment?			
E. Does the platform support future SaaS features or new applications?			
2. Backup and restore features			
A. Is backup data stored in hot storage?			
B. Can backup data be previewed before restore?			
C. Are restores granular and/or bulk?			
3. Storage and retention			
A. Does the platform ensure data is retained and protected?			
B. Can storage scale without additional fees?			
C. Can data residency be restricted to specific geographies?			

1. Backup and data protection

Use these questions to evaluate how well a vendor's backup solution covers your SaaS environment. Strong protection means extensive support across all critical data, immutability, and the agility to support future SaaS applications.

A. Which SaaS applications are supported natively?

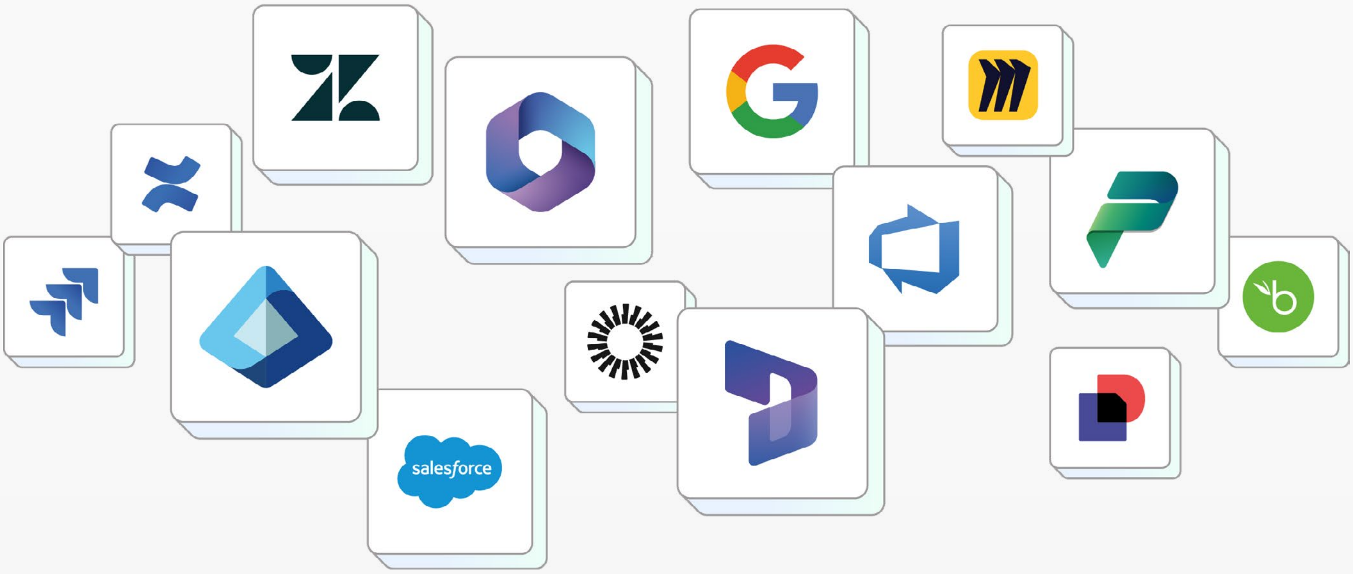
Look for broad coverage of your organization's core SaaS platforms to minimize manual setup and gaps in protection.

When evaluating backup vendors, consider breadth of coverage. SaaS now hosts critical business data — financials, HR files, customer records, and intellectual property — so backups should cover all key applications, not just a few major ones.

B. For each application, which data types are protected?

Confirm that both primary data and supporting elements — metadata, configurations, policies — are fully included in backups and restores.

When evaluating vendors, it's also essential to look beyond surface-level application coverage. The depth of protection matters just as much as the breadth. For every SaaS application, assess which data types are backed up and restorable — for instance, whether metadata, configurations, or policy information are included. Missing these elements can result in longer downtime and incomplete restores when you need your data the most.



C. Are backups immutable?

Ensure backups cannot be modified or deleted to help protect against ransomware and accidental data loss.
Immutable backups provide a critical safeguard by preventing any changes, deletions, or encryptions once data is written. True immutability ensures data remains in its original state for the entire retention period, regardless of user actions or malicious attacks.

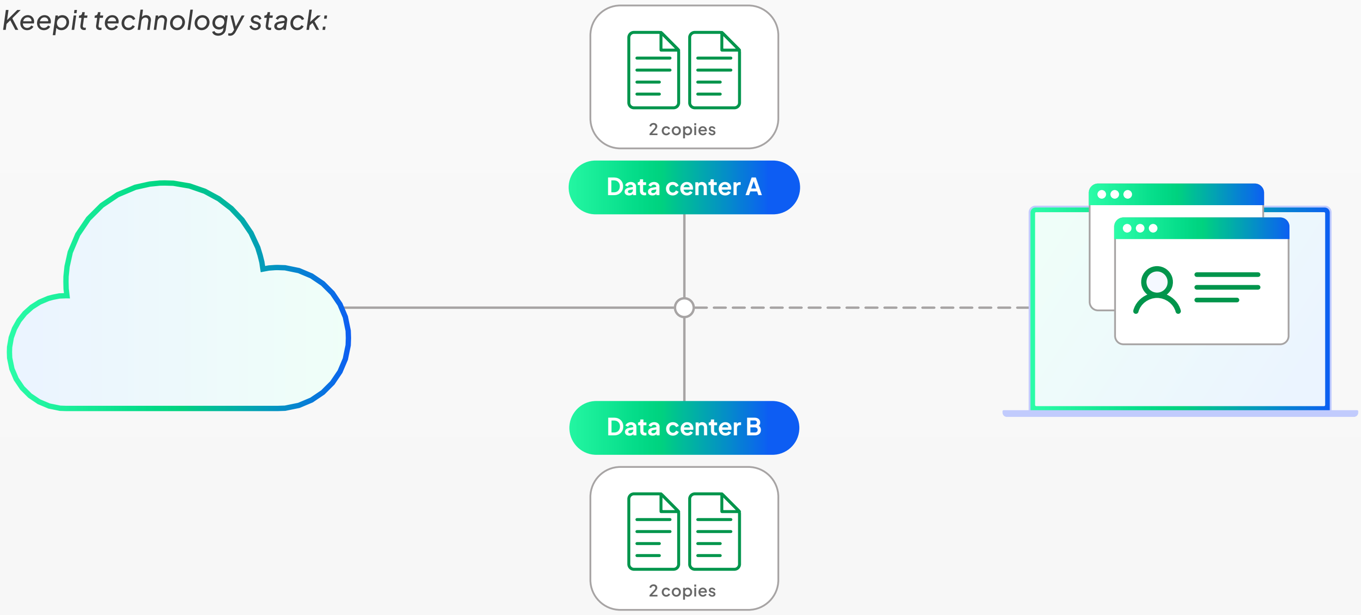
D. Are backups stored in an independent cloud environment?

Ensure data is stored independently from production environments for true air-gapped protection and ransomware resilience.
Make sure to ask where your backups will reside. Backing up data within the same SaaS provider's infrastructure doesn't reduce risk. Relying solely on the public cloud does not guarantee security or offer air-gapped protection, as backup data still sits within the shared infrastructure of the production system and thus remains vulnerable to systemic failures or ransomware events. Look for vendors that store backups in an independent, logically and physically separate cloud environment to ensure true air gapping and resilience.

E. Does the platform support future SaaS features or new applications?

Assess the vendor's roadmap and flexibility to quickly add new integrations and maintain comprehensive protection over time.
Finally, consider the vendor's future readiness. How easily can their platform adapt to new SaaS applications or evolving features within existing ones? A vendor's ability to extend coverage and enhance protection depth over time indicates long-term reliability and commitment to data resilience.

Keepit technology stack:



2. Backup and restore features

Use these questions to evaluate how effectively a vendor enables recovery of your SaaS data. Strong backup and restore capabilities mean data is continuously protected, easily searchable, and quickly recoverable — whether you need to restore a single file or an entire environment. Flexibility, accessibility, and speed are key indicators of a mature and resilient solution.

Learn more about common challenges during a recovery process and what an intelligent recovery process means in this Keepit's fact sheet.

A. Is backup data stored in hot storage?

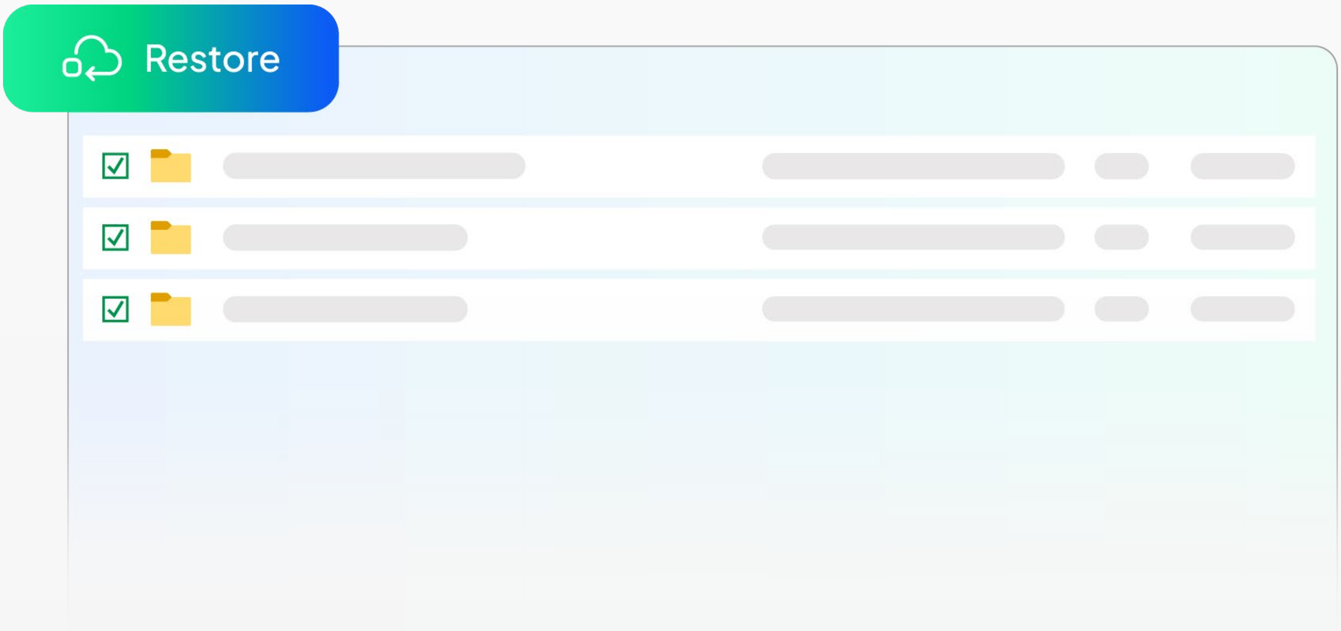
Evaluate how quickly backed-up data can be accessed.
Data stored in hot, fully indexed storage is available for immediate recovery, dramatically improving recovery speed and enabling you to meet your recovery time objectives (RTOs).

B. Can backup data be previewed before restore?

Assess whether users can preview or search through data before restoring.
The ability to preview or search through backed-up content ensures accuracy — users can confirm they're restoring the right item before committing changes. This combination of accessibility and precision underpins fast, confident recovery when every minute counts.

C. Are restores granular and/or bulk?

Assess whether the solution supports both granular and large-scale restores, e.g., from an individual item or folder to full mailbox, site, or tenant recovery.
Being able to select restore granularity is critical for meeting diverse recovery needs. The ability to restore a single file or email saves time in everyday user scenarios, while full-tenant recovery is indispensable during incidents such as ransomware attacks or accidental mass deletions. A solution that supports both granular and bulk restores ensures flexibility and minimizes downtime across different threat or failure situations.



3. Storage and retention

Use these questions to evaluate how a vendor manages the storage, protection, and retention of your SaaS data. Strong storage and retention capabilities ensure your data is securely preserved, compliant with regulations, and scalable as your organization grows — without unexpected costs or operational complexity.

A. Does the platform ensure data is retained and protected?

Assess the platform's security measures, architecture, and storage ownership. Look for protections such as immutability, encryption, redundancy, and a design that minimizes single points of failure.

Data retention and protection are foundational to business continuity and compliance. Understanding how a vendor structures its storage and safeguards data — for example, whether they manage their own storage or rely on third-party providers — helps you verify reliability, resilience, and control. Strong protections reduce the risk of data loss and ensure your backup solution can meet regulatory or organizational requirements.

B. Can storage and retention scale without additional fees?

Evaluate how storage usage is measured and billed. Determine whether costs increase with data growth or user count, and whether the vendor offers flexible, predictable pricing models.

Scalability without hidden fees is critical for growing organizations. If storage costs increase exponentially as your company or data grows, the solution can quickly become cost-prohibitive. Some backup vendors, for example, charge additional rehydration fees when hot storage is not included, creating unexpected costs. Buyers need to understand pricing models to ensure predictable budgeting while maintaining sufficient storage capacity for future growth.

C. Can data residency be restricted to specific geographies?

Check whether the vendor allows data to reside in specific regions or countries, as required for regulatory, legal, or corporate compliance, and note any restrictions, including no transmission guarantees.

Data residency is increasingly important for organizations with legal obligations around digital sovereignty or cross-border data flows. Restricting storage to specific geographies is key to supporting compliance with local laws, reducing regulatory risk, and may be required for highly sensitive data, such as healthcare, financial, or government information. Learn more about how to keep control of your data in our data sovereignty report.

D. How long is data retained?

Verify the platform's retention policies and limits, including whether long-term or unlimited retention is supported and how retention interacts with billing.

Retention period affects both compliance and cost. Organizations need clarity on how long data can be retained and whether this impacts pricing. Solutions that allow extended or unlimited retention provide long-term protection for critical records without forcing premature deletion or incurring unexpected fees.

4. Security and compliance

Use these questions to evaluate how a vendor protects your SaaS data and supports regulatory obligations. Strong security and compliance measures ensure that your backup solution not only safeguards data against unauthorized access but also helps your organization meet industry-specific requirements and demonstrate accountability.

A. Is MFA, SSO, and RBAC enforced for administrators and users?

Verify that the platform supports multi-factor authentication (MFA), single sign-on (SSO), and role-based access control (RBAC) to manage user access and permissions.
Strong access controls are a fundamental security requirement. Enforcing MFA, SSO, and RBAC reduces the risk of unauthorized access and helps maintain data integrity. For organizations with complex IT environments or strict internal policies, these controls provide confidence that only authorized users can perform sensitive backup and restore operations.

B. Are audit logs and monitoring available for backup and restore actions?

Assess whether the solution provides detailed logs and monitoring capabilities for backup and restore activities, enabling visibility into who accessed what and when.
Audit logs and monitoring are essential for compliance, accountability, and forensic investigations. Many industries — including finance, healthcare, and public sector — require evidence that critical data has been properly managed. A solution that maintains comprehensive audit trails ensures you can quickly demonstrate regulatory compliance or investigate security incidents.

C. Does the platform support compliance with legal and regulatory requirements?

Determine if the vendor helps meet industry-specific regulations such as HIPAA, GDPR, or other industry and regional requirements.
Backup solutions often play a key role in achieving regulatory compliance. By providing encrypted, immutable, and independent backups, the platform can support legal obligations around data protection, privacy, and retention. Understanding which requirements are addressed helps organizations mitigate risk and avoid penalties while ensuring operational continuity.

D. What certifications or compliance frameworks does the platform meet?

Check for recognized certifications and frameworks such as SOC 2, ISO 27001, or other relevant standards that validate the platform's security posture.
Certifications provide independent assurance that the vendor follows rigorous security practices. For highly regulated industries, choosing a solution with verified compliance frameworks reduces audit burden, builds trust with stakeholders, and demonstrates adherence to industry best practices.

5. Monitoring, reporting, observability

These questions help you evaluate how well a backup and storage platform allows you to track, analyze, and act on operational data. Monitoring and reporting capabilities are essential for proactively managing your environment, detecting anomalies, and maintaining overall system health. Use these questions to assess whether or not a vendor provides the insights and visibility your organization needs to stay in control.

A. Does the platform provide real-time monitoring/anomaly detection?

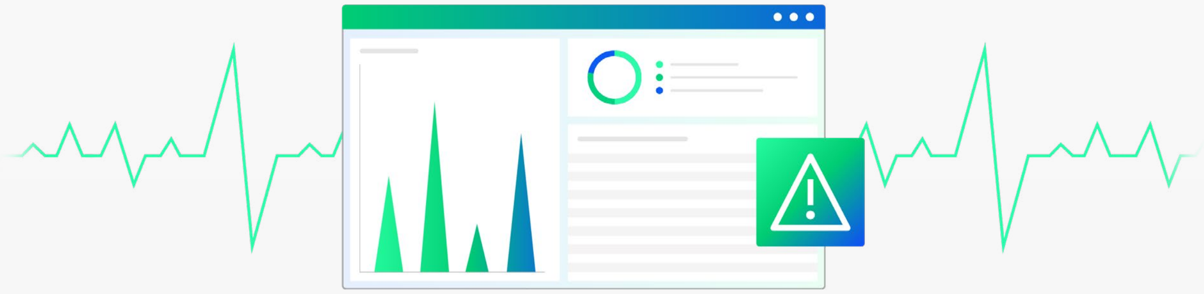
Ensure the platform provides tools to monitor data volume so you can respond quickly to suspicious activity. Real-time monitoring and anomaly detection empower teams to identify unexpected changes in backup data — such as sudden deletions, unauthorized modifications, or unexpected growth — enabling swift investigation and recovery. This proactive approach minimizes downtime, prevents data loss, and enhances overall system reliability.

B. Does the platform provide real-time monitoring of backup jobs and restores?

Assess whether or not the platform offers comprehensive visibility into all critical operations, from backups, snapshots, and restores. Having a complete, real-time overview ensures that your organization can track system health, confirm job completion, and quickly address operational issues. By also monitoring snapshot activity, you can verify data consistency and integrity at every point in time. This level of visibility keeps teams informed and reduces the risk of unnoticed failures or data loss.

C. Can status, progress, and alert data be exported or integrated with SIEM and CIEM tools?

Check if the platform allows exporting data or integrating it with security information and event management (SIEM) and cloud infrastructure entitlement management (CIEM) tools. Integration and export capabilities enable organizations to centralize monitoring, correlate backup data with other security events, and streamline compliance workflows. This ensures that security teams can act on anomalies quickly, maintain audit readiness, and strengthen overall risk management.



6. Vendor capabilities and reputation

These questions help you evaluate whether a vendor has the experience, scale, and reliability to support your organization over the long term. Understanding a vendor's background, customer success track record, and operational footprint ensures you can partner with a company that is not only capable today but will continue to innovate and provide support in the future. Use these questions to validate expertise, stability, and trustworthiness.

A. Was the vendor built for the cloud from the start?

Focus on whether or not the vendor is cloud native and designed specifically for SaaS environments rather than starting with on-premises backup and later adapting to the cloud.
Vendors that were built for the cloud from the beginning tend to have deeper expertise, more mature processes, and solutions optimized for cloud environments. This reduces risk compared with vendors that started on-premises and are now retrofitting their offerings for SaaS backup.

B. Are industry recognition, analyst coverage, or case studies available?

Request awards, certifications, analyst reports, and relevant customer case studies. These validate the vendor's reputation, market leadership, and ability to deliver in similar organizations or industries.
Industry recognition and analyst coverage help validate the vendor's market reputation, demonstrate their ability to meet industry standards, and give confidence that the solution is widely respected and trusted in the sector.

C. How frequently are new SaaS applications supported or added?

Assess how actively the vendor expands its coverage for new SaaS applications.
Frequent updates indicate a vendor's commitment to keeping pace with the evolving SaaS ecosystem. This ensures that you can rely on them for future needs as your organization adopts additional cloud applications.

D. Where is the vendor headquartered, what types of support does the vendor provide, and how accessible are they?

Check the location of the vendor's offices and their support offerings.
Knowing the vendor's headquarters gives insight into operational footprint and legal jurisdiction, while understanding support types and accessibility helps assess responsiveness, service continuity, and overall customer experience.

Bringing it all together

Collect vendor responses, assign a score for each question, and total the results to get a clear picture of each vendor's level. This structured approach helps you move beyond marketing claims and assess who can truly support resilient, compliant recovery.

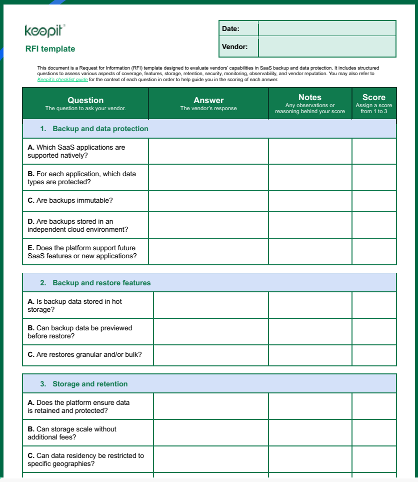
Organizations that consistently use this checklist as part of vendor evaluations not only improve visibility into their SaaS resilience but also accelerate their journey toward the managed stage of the disaster recovery maturity framework, where DR is owned by leadership, integrated across functions, and continuously improved.

Because in the end, disaster recovery isn't just about reacting to disruption; it's about managing resilience as a strategic advantage, no matter which challenges arise.

Not sure where to start? Book a resilience readiness consultation with Keepit to assess how well your current SaaS backup strategy protects you against data protection gaps, compliance risks, and ransomware threats.

Get the RFI template and use it to evaluate vendors

Download now



keepit

RFI template

Date:	
Vendor:	

This document is a Request for Information (RFI) template designed to evaluate vendors' capabilities in SaaS backup and data protection. It includes structured questions to assess various aspects of coverage, features, storage, retention, security, monitoring, observability, and vendor reputation. You may also refer to Keepit's checklist guide for the context of each question in order to help guide you in the scoring of each answer.

Question The question to ask your vendor.	Answer The vendor's response	Notes Any observations or reasoning behind your score	Score Assign a score from 1 to 3
1. Backup and data protection			
A. Which SaaS applications are supported natively?			
B. For each application, which data types are protected?			
C. Are backups immutable?			
D. Are backups stored in an independent cloud environment?			
E. Does the platform support future SaaS features or new applications?			
2. Backup and restore features			
A. Is backup data stored in hot storage?			
B. Can backup data be previewed before restore?			
C. Are restores granular and/or bulk?			
3. Storage and retention			
A. Does the platform ensure data is retained and protected?			
B. Can storage scale without additional fees?			
C. Can data residency be restricted to specific geographies?			

keepit®

Your data. Here today. Here tomorrow.

Keepit provides a next-level SaaS data protection platform purpose-built for the cloud by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience, and future-proof data protection. For more information visit www.keepit.com or follow Keepit on LinkedIn.

bsi ISO/IEC 27001 Information Security Management CERTIFIED