# Data Protection Best Practice Guide

ASSESS & DESIGN – STAGE 1

Backrightup
WWW.BACKRIGHTUP.COM | SYDNEY, AUSTRALIA

Backrightup

# Contents

# Backrightup Data Protection Best Practices – Assess & Design

Welcome to the Backrightup Data Protection Best Practice Guide – Assess & Design. This resource is designed to offer best practices for optimizing and designing the use of Backrightup Data protection. While it does not serve as a comprehensive documentation or detailed feature explanation, you can find other supporting information in the Backrightup Knowledgebase.

This guide is the first stage in a two-stage process:

1) Assess & Design
2) Configure, Operate & Secure

Primarily aimed at professionals seeking insights and recommendations on various topics, this guide covers design ideas, optimal feature utilization, potential pitfalls to avoid, and more. The content is a culmination of practical knowledge developed, gathered, and regularly updated by our team of Backrightup Consultants, who actively engage with our Backrightup customers in real-world scenarios. Rather than delving into theoretical aspects, the focus is on practical application.

It's important to note that while best practices typically suit the majority of cases, they may not be universally applicable and could be incorrect under specific circumstances. Understanding the implications of recommended practices is crucial. If uncertainties arise, feel free to reach out to Backrightup professionals through our support email at support@backrightup.com.

Based on the design outcomes of this document, Backrightup will provide the recommended configuration guides for the Configure, Operate & Secure stage.

## 1. How to use this guide

The basic idea is to resemble the same workflow that a Backrightup consultant would follow when implementing a new instance of Backrightup:

**1-Assess & Design (Stage 1):** First, you start by understanding the current Azure DevOps environment. You should collect the data and:

- Understand the levels of acceptable risk requirements from the business and stakeholders.
- Understand existing SLA's, RPO and RTO and all the other information that is needed to design the solution.

- Understand the requirements for business continuity for the business and the SLA's regarding this continuity.
- Understand where data should ideally be stored.
- Understand where ideally the data should be geographically processed and redundancy requirements.
- Understand how the organization will manage users in the application, the roles of these users, onboarding and offboarding procedures, and managing access to the platform.
- Understand how the organization will manage restore testing for compliance with standards such as ISO27001 / SOC 2 procedures.

With all the information that has been collected, you start to design the solution, by involving all the required Backrightup components and/or external storage components, each with their characteristics, strengths, and limits, and you will also learn how to properly configure them, with security always in mind.

**2-Configure (Stage 2):** Once the environment has been designed, it's time to build it. A DevOps specialist can configure it themselves or pass the instructions to other teams to proceed with the deployment. Alternatively, please book a time with a Backrightup specialist to chat and confirm configuration options.

**3-Operate (Stage 2):** When the environment is ready, it's time to use it! Here, you will learn how to properly configure the different jobs available in the software and how to restore data.

**4-Secure (Stage 2):** When you have been through all the other stages, it's time to make sure you have as little risk as possible. This section covers basic security principles that would help reduce risk and give extra confidence in your Backrightup project. When you are here, you should always go back to the start to ensure you have achieved your objective. We have assumed you will iterate naturally and from time-to-time fine tune to reach your goal.

# 2. Assess & Design

The basic idea is to resemble the same workflow that a Backrightup consultant would follow when implementing a new instance of Backrightup:

## 2.1 Levels of Acceptable Risk Expectations

The perfect backup solution should ensure the integrity of the backed-up data. There should be minimal risk of data corruption or loss during the backup and restoration processes.

Stakeholders may expect that data can be recovered without any compromise to its accuracy or consistency.

However in a backup of any SaaS solution data, there are few limits to restore imposed by various factors such as Vendor API limits/restrictions, relationships between entities and

other internal workings of the vendor itself; in our case Microsoft and GitHub.

As an example, Backrightup will recover the following elements (please note this list is not exhaustive – please request an exhaustive list from Backrightup):

| Entity | Requirements | Comments |
|---|---|---|
| **Projects** | Organization must exist | |
| **Repositories** | Project must exist | - Repos are restored with new Id<br>- Repos can be restored together with Pull Requests if required via UI |
| **Pull requests** | Repository must exist to restore pull requests | - Pull request will be restored with new Ids |
| **Work Items** | Requires correct process template to be restored.<br>Requires correct area/iteration group to be restored | - For accurate restore, the "Boards" restore in Backrightup will attempt to create the area groups and iterations in the new group<br>- Work items will be restored with new Ids<br>- Work items together with correct |
| **Area groups/iterations** | Project must exist | Restored with new internal Ids |
| **Processes** | Organization must exist | Restored with new internal Ids |
| **Builds** | Repository must exist | Restored with new internal Ids |
| **Releases** | Repository must exist | Restored with new internal Ids |
| **Variable groups** | Project must exist | Restored with new internal Ids |
| **Task Groups** | Project must exist | Restored with new internal Ids |
| **Artifacts** | Project must exist | Restored with new internal Ids |

The requirements for these entities to be restored are documented in the table above. Generally, Backrightup will execute a "create" process when restoring, recreating the entities via the Azure DevOps API, private API's provided to Backrightup via Microsoft or in some cases manually from backup files when required.

Although this process enables business continuity, the previous Id's, custom extensions, users and/or permissions may or may not be available depending on the entities restored and order of restore.

Our extended restore support is another service (documented below) which is available to assist in running restores when required to ensure that the maximum amount of data can be restore – recreating this data via the UI if required.

Risk can further be mitigated by considering the following options:

1) Regular Restore Testing.
2) Extended Restore Support.

Regular Restore Testing

Regular restore testing may already be part of the processes followed for your BCDR. In some scenarios, regular restore testing may be required to comply with ISO27001 or other standards boards. Reducing business continuity risk starts with ensuring that your company can initiate and complete a restore successfully and the data recovered is acceptable to the business.

Backrightup also offers a done-for-you service restore testing service on a monthly basis where the results of your project restore, the entities restored and associated analytics are provided to ensure that BCDR Compliance is met and in the worst-case scenario, restore from backup can be performed.

Extended Restore Support

In the worst-case scenario your company wants to be sure that you can restore effectively and return to normal as soon as possible. Backrightup offers a team of support engineers qualified in advanced restores to assist in returning the DevOps organization back to full working order as soon as possible. The restore team use any means possible (manual restore from Json backup blobs, to Azure DevOps API's when required) to return the project to normal working order.

Use of this service further reduces your overall risk but having experts on-hand as well as the recovery time objective (discussed in 2.2 below).

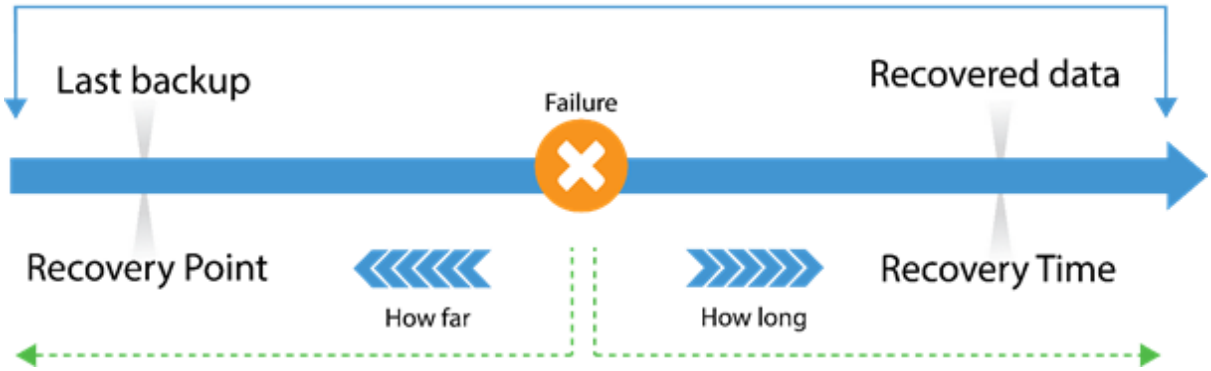
## 2.2 Business Continuity and Disaster Recovery Plan (BCDR)

Two critical parameters that play a key role in defining a BCDR plan include the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO):

**RPO** establishes the temporal limit for data rollback, specifying the maximum acceptable data loss measured from the occurrence of a failure to the time of the last valid backup. To illustrate, in a banking system where real-time transactions are crucial, an hour of data loss can have catastrophic consequences. On a personal level, envision the RPO as the point at which you last saved a document you are actively working on. If a system failure occurs and your progress is lost, consider how much work you are willing to forfeit before it significantly

impacts you.

On the other hand, the **RTO** is linked to downtime and signifies the duration required to restore operations from the incident until normal functionality is accessible to users.




By default, RPO for Backrightup is 24 hours due to the default setting of daily backups. RPO can be set as low as 4 hours on the Backrightup Enterprise Plan. Please advise the Backrightup team should you wish to lower the default RPO.

By default, RTO can vary from 5 minutes to multiple days due to the size of the entity being restored, the number of items restored, API rate limiting restrictions from Microsoft and other network or environmental issues. During large restoration requests, our service is able to scale out to process data more efficiently and therefore restore times cannot be extrapolated linearly. To help you and the team define your RTO, we have given some guidelines for different entities:

Repositories:

5MB ~ 3 minutes total restore time
100MB ~ 7 minutes total restore time

Work Items:

10 work items ~ 5 minutes total restore time.
20 work items ~ 5 minutes total restore time.
100 work items ~ 7 minutes total restore time.
1000 work items ~ 30 minutes total restore time.

All other entities (e.g. Shared queries, releases, builds etc):

1 item ~ 5 minutes

## 2.3 Authentication & Single Sign-On (SSO)

At this point you should consider the requirements for sign on to the Backrightup platform. Backrightup supports 4 separate options:

1) **Username/Password (not recommended)**
   When signing up for Backrightup, you may elect to use Username/Password combination. Although the standard password length must adhere to at least 8 characters, this method does not support a second factor which puts your account at risk in the event of an exposed or simple password.

2) **Username/Password (with MFA)**
   Similar to the above method, except that MFA may be enabled to further protect the Username/password combination. On login using the username/password combination, Backrightup will prompt for a token that must be generated by an authentication app such as Duo or Microsoft Authenticator.

3) **Single sign-on linked to Microsoft Entra ID/Google Workspace/GitHub**
   Electing to use your Microsoft Account linked to Entra ID will allow your team to inherit the permissions and authentication methods used by your Company. Backrightup will redirect to your company's Entra Id instance and request authentication before passing back to Backrightup for login. All authentication mechanisms enabled within your Entra ID tenant (e.g. multi-factor authentication/) will be used.

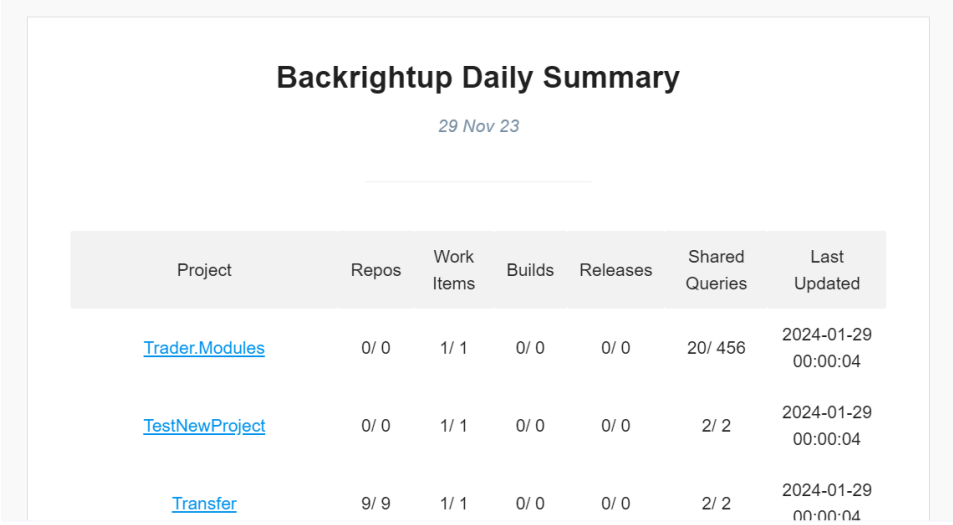
4) **Okta Single sign-on**
   Okta authentication may also be used by your company to authenticate to your instance. Please consult a Backrightup consultant for more information about adding the Backrightup application to your Okta instance.

Consider which sign on mechanism best fits the organization before proceeding to signup for Backrightup to ensure your data remains secure.

## 2.4 Backup Email Summaries

Backrightup will send 2 types of email summaries:

- Daily Summary – all items backed up across per product (Azure DevOps + GitHub) per day.

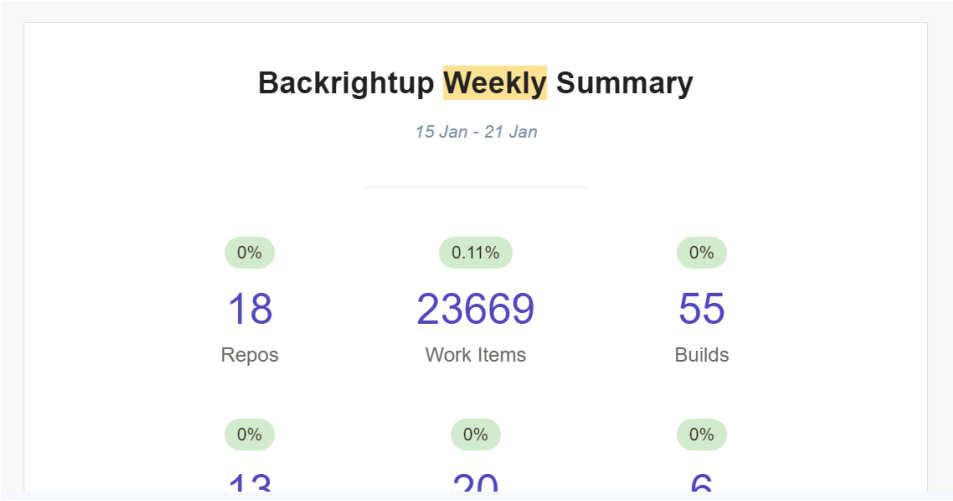


**Backrightup Daily Summary**

*29 Nov 23*

| Project | Repos | Work Items | Builds | Releases | Shared Queries | Last Updated |
|---|---|---|---|---|---|---|
| Trader.Modules | 0/ 0 | 1/ 1 | 0/ 0 | 0/ 0 | 20/ 456 | 2024-01-29 00:00:04 |
| TestNewProject | 0/ 0 | 1/ 1 | 0/ 0 | 0/ 0 | 2/ 2 | 2024-01-29 00:00:04 |
| Transfer | 9/ 9 | 1/ 1 | 0/ 0 | 0/ 0 | 2/ 2 | 2024-01-29 00:00:04 |

- Weekly Summary – a summary of all items backed up and not backed up



**Backrightup Weekly Summary**

*15 Jan - 21 Jan*

| | | |
|---|---|---|
| 0% | 0.11% | 0% |
| 18 | 23669 | 55 |
| Repos | Work Items | Builds |
| 0% | 0% | 0% |
| 13 | 20 | 6 |

Summaries can be sent to multiple stakeholders and systems. Please consider at this point which system or stakeholder would be best to receive each of these types of emails. This decision may be reached in consideration of the below 2.5 Backup Alerts/Webhooks given that the alerts may be consumed by a backup monitoring solution used by the entire enterprise.

## 2.5 Backup Alerts and Webhooks

An organization managing any number of backups may run a system to monitor these alerts such as Azure Monitor, Splunk, PagerDuty, Backup Radar or similar. Backrightup can be configured to send alerts via webhooks to the relevant system

Contact your IT Management team to consider whether these notifications should be implemented, and which system should be receiving these alerts.

## 2.6 Backup Locations and Redundancy

The fundamental principle in data protection and redundancy is encapsulated by the 3-2-1 rule. This essential guideline advises maintaining:

- Three copies of the data (2 copies and the data itself in production)
- Stored on two distinct media (if possible)
- With one copy located off-site (potentially offline)

When strategizing for the backup of Azure DevOps, it is imperative to incorporate these rules into your planning. The chosen storage architecture for your Backrightup Azure DevOps Backup infrastructure will determine various strategies to align with the 3-2-1 design guideline.

Backrightup provides options to store a primary backup AND secondary backup (and therefore fulfilling the 3-2-1 rule) in one the following locations:

| Name | Owned by | Type |
|---|---|---|
| South Central US | Backrightup | Azure |
| Azure blob + table storage | Customer | Azure |
| AWS S3 storage | Customer | AWS |
| Wasabi S3 Storage | Customer | Wasabi |
| SFTP Storage | Customer | SFTP |

For companies considering Azure storage, we recommend the current Best Practice Guide from Microsoft together with georedundancy storage.

For companies considering AWS storage, we recommend the current Best Practice Guide from Amazon Web Services together with georedundancy storage.

For companies considering Wasabi storage, we recommend the current Best Practice Guide from Wasabi.

In the event SFTP storage is selected, please be aware that the availability of the storage endpoints will be your responsibility. If you are attempting to implement on-prem storage via SFTP, we recommend consulting the Backrightup team to establish connection testing and approval.

All backups are 256-bit encrypted and must be restored via Backrightup. Consider which storage media is best for your implementation to mitigate risk.

Ensure that your S3 (AWS & Wasabi) clients are using HTTPS transport, i.e. The URL contains “https” as in the example of https://s3.us-east-2.wasabisys.com/.

By default, Backrightup encrypts each storage object using a random Advanced Encryption Standard (AES) 256-bit key.  The key is stored in an Azure Key Vault meta-data secure layer of

the Backrightup system (until the object is deleted) and is used again for decryption when the object is retrieved.

## 2.7 Backup IP Restrictions and Bring-Your-Own-Key (BYOK)

If you elect to use your own storage, Backrightup can further secure access to your backups by supplying a static/finite set of IP addresses for which you may ALLOW to your storage.

As a further security precaution, Backrightup also allows customers to bring their own encryption keys which can be used to further encrypt the data when processing the backup data. These keys are of course stored in an encrypted state in a separate key vault to ensure separation of concern.

## 2.8 Data Sovereignty

Data Sovereignty is an important issue for many companies assessing backup solutions. Backup solutions will most commonly have a two separate points of work:

1) Data Processing
2) Data storage

Backrightup can ensure that both points (processing and storage) are geo-locked to a certain country or region as detailed in the architecture diagram below. The following regions/areas are currently supported:

1) West Europe (conforming to GDPR requirements)
2) South Central US
3) Australia East
4) UK South

For global companies, with offices in Europe, the best option is usually West Europe to ensure GDPR compatibility.

The location chosen by your organization does not have any meaningful bearing on processing times.

# 3. Backrightup High-Level Architecture