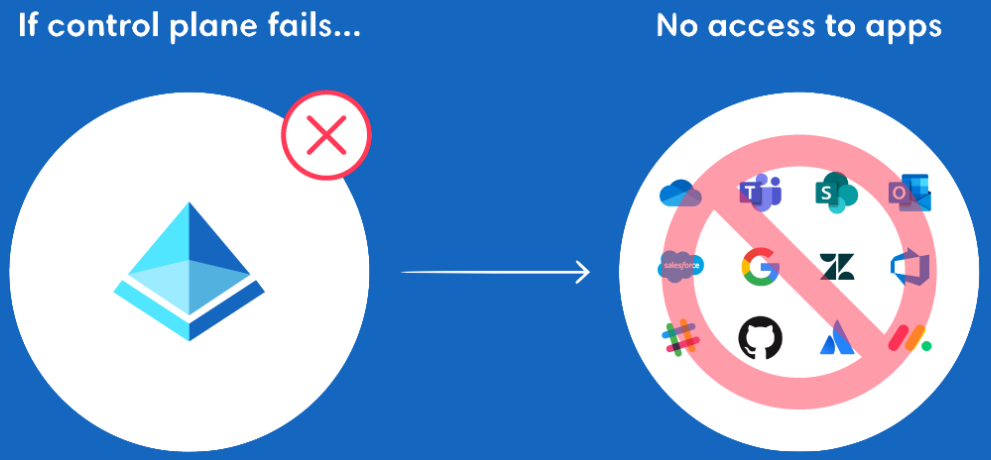
keepit®

July 2023

Risk assessment form:

Assess your need for Entra ID backup



Assess your need for Entra ID backup

This risk assessment sheet is a risk analysis tool that gives you a quick view of Entra ID risks and their consequences' severity (impact).

You use it to allocate ratings for each risk based on two intersecting factors:

- **The likelihood** (or probability) of a risk to occur
- **The impact** (or severity) if a risk occurs

The higher a risk ranks for these two factors, the bigger threat it poses to your project.

keepit

How to use the risk assessment sheet?

We've compiled a list of security risks (see pages 6-7) that your Entra ID environment may face without a backup.

To assess your risk level, follow these 3 steps for each risk:

1. **Determine likelihood (page 4):**
   Identify the chance of each risk occurring using the likelihood scale on the next page. Write your rating on page 6-7 in the likelihood column.

2. **Define impact scale (page 4):**
   Rank risks based on the impact they would have on your company using the impact scale on the next page. Write your ratings on page 6-7 in the impact column.

3. **Calculate risk rating (page 5):**
   Assess likelihood and impact to calculate a risk rating for each risk using the equation: Likelihood x Impact = Risk rating. Ratings range from 1 to 25 (see scale on page 5) and aid in determining the need for Entra ID backup. Write your ratings on page 6-7 in the risk rating column.

   A higher number of medium and high-level risks indicate a greater necessity for Entra ID backup.

keepit®

Likelihood scale

LIKELIHOOD	DEFINITIONS
1	**Very unlikely:** A very slim chance for this risk to occur.
2	**Not likely:** Low chances for this risk to occur.
3	**Possible:** Fifty-fifty chances for this risk to occur.
4	**Probable:** Good chances for this risk to occur.
5	**Very likely:** You can bet this risk will occur at some point.

Impact scale

IMPACT	DEFINITIONS
1	**Negligible:** This risk will hardly impact your business.
2	**Low:** You can easily handle the consequences of this risk.
3	**Moderate:** It will take some time and effort to mitigate the consequences of this risk.
4	**Significant:** This risk could cause long-term consequences that will be hard to recover from.
5	**Catastrophic** The impact of this risk might wreck your business.

keepit

Risk rating (= Likelihood x Impact)

1 – 6 (Low): Low-rating risks most likely will not happen. If they do, they will not be a threat to your organization.

7 – 12 (Medium): Some medium-rating risks might happen at some point. You do not need to prioritize them but you should not ignore them either.

13 – 25 (High): High-rating risks are serious and very likely to happen threats. They can cause your organization to go off the rails, so you should keep them in mind when planning your Entra ID security.

keepit

Fill in the risk assessment form to assess your need for Entra ID backup

RISK	RISK DESCRIPTION	LIKELIHOOD	IMPACT	RISK RATING	RESPONSE
Loss of security / configuration policies	Entra ID allows administrators to define and enforce various configurations, policies, and access controls. Not having a backup means the loss of these settings, which can result in inconsistencies, misconfigurations, and unauthorized access. It may take significant time and effort to recreate and reapply these configurations, leaving the environment exposed to potential security risks.				With a backup of Entra ID organizations have more control over the restoration process, as they can easily recover permanently deleted cloud objects like device configurations, security policies, and access controls in a fast and efficient way.
Limited recovery options	Entra ID provides native features for data recovery, such as recycle bin and soft delete options. However, these options may have limitations, such as time-bound retention or inability to restore specific attributes or configurations.				A proper backup of Entra ID ensures more comprehensive recovery options and greater control over the restoration process.
Failure to meet compliance requirements	Organizations are often subject to various regulatory requirements, such as GDPR or industry-specific regulations. Failure to have a backup of Entra ID can lead to non-compliance with data protection and privacy regulations, resulting in potential legal issues, financial penalties, and reputational damage.				A backup of Entra ID ensures continuous chain-of-custody and provenance of security policies. This allows organizations to prove to regulators exactly what policies were in place at any time and document changes and deviations, if any

keepit

Fill in the risk assessment form to assess your need for Entra ID backup

RISK	RISK DESCRIPTION	LIKELIHOOD	IMPACT	RISK RATING	RESPONSE
Data loss	Entra ID stores security policies, application settings, and other cloud-only configurations. If this data is lost due to accidental deletion, malicious activity, or system failure, it can lead to severe consequences, including user access issues, operational disruptions, and compliance violations.				If you have a backup before the incident, you can use it to easily recover your lost data and bring it back into your Entra ID environment right away.
User productivity impact	Without a backup, recovering security and device policies can be a difficult and time-consuming task. This process may restrict activity or even prevent users from logging in to apps.				Restoring security policies and configurations manually can result in significant downtime and decreased productivity for users who are unable to access the resources they need.
Microsoft system outages	If Entra ID experiences a prolonged outage or catastrophic failure, organizations without a backup will have limited options for recovery, leading to extended periods of system unavailability, and business disruption.				No backup can prevent Microsoft from having a system outage, that's simply a risk all organizations face. However, if you have a backup, you can use it to recover your data once the service outage is resolved.

keepit

Why Keepit is the best backup & recovery for Entra ID

- Broadest coverage on the market
- Back up cloud objects not covered by the Recycle Bin
- Extend the retention and the ability to recover Entra ID objects
- Ability to selectively roll back changes
- Preserve important records for compliance purposes
- Recover lost data in disaster scenarios
- Increase IT efficiency

Read more about Keepit's Entra ID backup here

Leading protection

Coverage:	keepit	Quest	AvePoint	metallic	Active Directory
Azure AD (Entra ID) Standard Free					
Users	Yes	No	Yes	Yes	Yes
Groups	Yes	Yes	Yes	Yes	Yes
Admin Units	Yes	No	No	No	No
Roles	Yes	Yes	No	No	No
Azure AD (Entra ID) Advanced					
Audit logs	Yes	No	Yes*	No	Yes
Sign-in logs	Yes	No	No	No	Yes
CA policies	Yes	Yes	No	No	No
App registrations	Yes	No	Yes	Yes	Yes
Service principals/Enterprise apps	Yes	Yes	Yes	Yes	No
Intune device compliance policies	Yes	No	No	No	No
Intune device configuration profiles	Yes	No	No	No	No
BitLocker recovery keys	Yes	No	No	No	No
Contacts	Coming soon	Yes	No	No	No
MFA settings	No	Yes	No	No	No

*Audit logs available with an additional different product

CUSTOMER TESTIMONIAL

Our normal traditional backups for Azure Directory aren't necessarily covered by any Azure AD backup...

Now that we have Keepit, we are covered. No data loss, no user downtime. If we needed to, we could get back up and running at a very short period of time

Ken Schirrmacher,

Chief Technology Officer

PARK 'N FLY®

keepit

Entra ID (Azure AD) and M365 are better together —

Get complete protection for your entire Microsoft cloud with Keepit

+

keepit

Get Entra ID (Azure AD) backup
for free today.
Sign up here.