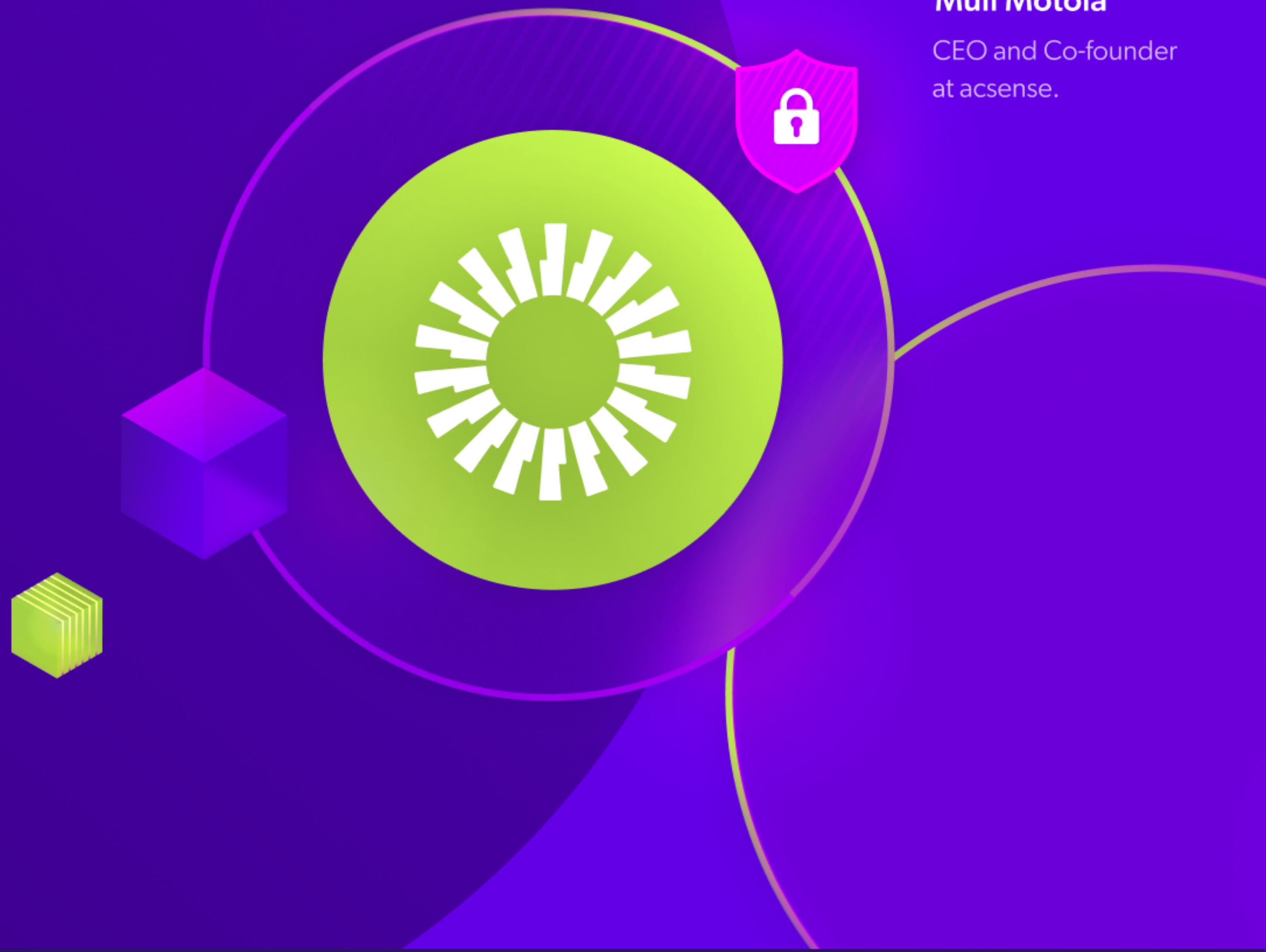
acsense

Barry Gordon

Head Coach & Founder
at Identity Coach

Muli Motola

CEO and Co-founder
at acsense.



THE OKTA

DISASTER RECOVERY PLAN GUIDEBOOK

The ultimate guide to crafting an Okta recovery plan on any budget.

Table of Contents

Overview

IAM solutions are growing in popularity, with over 75% of organizations using one. Okta is the IAM solution of choice for many of these organizations due to its excellent track record. While Okta ensures platform availability and resilience, the customer is responsible for ensuring the integrity of their configurations and data.

Failing to ensure data and configuration means organizations are vulnerable to disasters. To prepare for these disasters, organizations should consider how to implement overall IT infrastructure resilience. This is especially true for mission-critical assets.

When data or configurations are left exposed, organizations become vulnerable to threats from misconfiguration, malicious insiders, or external bad actors with compromised credentials. Since a company's IAM system is a critical operational component, companies cannot afford a lockout, loss of application access, or breach of essential assets. In fact, the average data breach costs companies 4.24 million dollars according to Abdalslam.com.

Effectively planning for a disaster is a crucial task that businesses must complete to minimize costs, downtime, and loss of security associated with a disaster. Yet, there is no one-size-fits-all solution to disaster planning. Every organization has its own unique business needs. These needs should influence the disaster plan strategy and the possibility of Okta inaccessibility.

One option for disaster planning is to develop internal recovery automation. However, this option often yields a costlier and less robust solution than commercial enterprise-grade tools. Nevertheless, internal recovery automation may be viable if your organization's needs are simpler, your budget is limited, or your business can still operate with extended downtimes. Preparing for a disaster is critical regardless of your organization's needs, budget, size, or essential assets.

Developing a Disaster Recovery Plan (DRP) is the first step in preparing for disaster. In this guidebook, you'll learn the necessary steps for creating a DRP and how to tailor your DRP to meet business needs. Whether you're a beginner or an expert, this guide will provide the tools and techniques you need to create a Disaster Recovery Plan.

Determining Recovery Scope

The first step in building a Disaster Recovery Plan (DRP) is to determine its scope. The scope of a DRP should handle such concerns as communication planning, user accounts, authentication strategy, application access, privileged access, maintaining backups, and disaster training. To create your DRP's scope, consider the following questions:

- In the event of a disaster, what parties must be informed?
- What information needs to be communicated to these parties?
- What is the best method of communication for each party?
- Do all IT infrastructure applications have to be accessible?
- What are the most critical applications for business needs?
- How will user authentication be handled?
- What is your organization's risk tolerance for temporarily disabling MFA?
- Which supporting identity, access workflows, and processes must continue even in a disaster?
- What is the Recovery Time Objective (RTO)?
- How old is the data required to return to business as usual?
- What are the time intervals for backups and retention?
- What is your organization's Recovery Point Objective (RPO)?
- Do you have any penalties if you do not meet service goals?
- Are key personnel trained in handling a disaster?
- How often will business needs and the disaster plan change?

Answers to these questions will yield the foundational building blocks for your DRP. Keep your answers to the above questions in mind as you read this guidebook to help determine the relevant, customized, and appropriate approach for each section of your Disaster Recovery Plan.

Communication Planning

After creating the scope of your Disaster Recovery Plan, the next step is to create a communications plan. This communications plan ensures that all necessary parties are informed and updated during a disaster. An effective communications plan should identify three key items.

1. Who should be notified in the event of a disaster
2. What information should be shared with them
3. How should this information be shared

The first step of communication planning is identifying the parties who should be informed of the disaster. To create this list, consider all the customers, employees, stakeholders, and other businesses who may be affected by the disaster.

Next, consider what information the parties in step one require. For example, employees will have different questions and concerns during a disaster than a customer. Information that should be shared can include changes to login processes, user credential updates, walk-throughs, or recovery steps for system administrators. After determining what information should be shared, it is time to evaluate how that information should be shared.

The method of communication is just as important as the content of the communication. Common methods used by organizations include email, SMS, the company website, and portals. In some instances, a phone call may be necessary. Whatever communication method is chosen, it should be strategic, efficient, and effective for the desired audience.

After creating a communications plan, it is paramount to schedule regular reviews of the plan to update content as needed. The communications plan is not a static document. It should evolve with an organization to ensure essential critical information is effectively delivered to the proper parties during the disaster recovery process.

User Account Backups and Restores

Having a recovery time objective (RTO) is an essential part of the DRP. To ensure the RTO is achievable, a strategy is needed to populate and sync user accounts into a recovery tenant. There is no one-size-fits-all solution to adding and maintaining user accounts in a recovery tenant. Common solutions for adding and maintaining user accounts in a recovery tenant are summarized in the following table. Check it out to determine what might be the best fit for your organization:

Method	Description	Pros	Cons
Ad Hoc	Manually add users to the recovery tenant	Simple Best for small user populations	Time-consuming Tedious Users must repeat enrollment to ensure credentials are updated
Directory Integration	Utilize external user directories (such as Active Directory) to quickly import users into a recovery tenant. If the recovery tenant is in standby mode, integrate the directory in advance to ensure the Okta directory is always up to date.	Password preservation Efficient and quick	Adds complexity Directory must have its own DRP and be available for recovery
Bulk & Scripted User Imports	Utilize delimited files of user data for bulk import into Okta. Ongoing and automated user data imports can be scheduled and scripted using the Okta Users API as part of the Okta tenant recovery. Be sure a plan for the first login post-disaster is included in the DRP.	Flexible Can be partially or fully automated User data can be backed up offline.	Does not preserve passwords or MFA enrollment if done by copying users from an Okta tenant directly or exporting them as JSON

Authentication Strategy

A user authentication strategy is a necessity after a disaster. There are a range of options when it comes to authentication strategy. To choose the appropriate method, consider business needs and operational requirements.

Multi-factor Authentication

Using the right strategy for handling Multi-Factor Authentication post-disaster is essential. The appropriate Multi-Factor Authentication strategy can ensure user access to critical assets during a disaster. Depending on disaster circumstances, some factors might be unavailable even if previously enrolled. In some cases, secondary authentication factors may not be enrolled in the recovery tenant. Prepare for your disaster recovery by choosing one of two options:

1. temporarily disable MFA
2. implement high-volume enrollment.

Temporarily Disabling MFA is the simplest route, though it is a high-risk option. This option allows users to access applications without MFA while the Okta tenant is being restored. MFA enrollment is then implemented in the recovery tenant process. To mitigate the risks of this method, consider disabling MFA for only some applications based on business needs.

Implementing high-volume enrollment is a lower-risk option than temporarily disabling MFA. Consider how quickly a user can set up a user MFA during a disaster. Since time is money, this option provides a time-sensitive and safer approach to handling Multi-Factor Authentication. Integrating a communication plan for high-volume MFA enrolment in the Disaster Recovery plan ensures this option can be easily enacted when disaster strikes.

Single Sign-On Failover

Ideally, Single Sign-On can be a failover for applications. However, a standby recovery tenant and applications supporting multiple Identity Providers (IDPs) are needed. When onboarding and amending applications, their configuration must be copied to the recovery tenant. This provides a cost-effective approach to retaining user experience during the disaster recovery process. Another option is to manually prepare a handful of critical applications that can be migrated to the recovery tenant. The steps for this manual migration should be documented to ensure a smooth recovery.

Directory-based Authentication

Active Directory and other directories are often designed to support high availability. Some organizations invest in IT infrastructure, allowing them to maintain directories during a disaster. Another option is a cloud-based solution like Azure Active Directory. These options can be a viable solution for failing over single sign-on for applications with directory integration.

Organizations with an Okta recovery tenant can also use Okta's LDAP interface. This can be an even more viable option than those listed previously. However, it requires applications to be configured in advance so they can be migrated quickly.

If using Okta's LDAP interface, be aware that traditional directories and Okta can be vulnerable to identical threats. Depending on how closely Okta and your Directory are coupled, a compromised Okta tenant may also mean a compromised directory. Plan for this contingency.

Local Application Authentication

Not every application can utilize Single Sign-On or directory integration for a seamless failover. In this case, user accounts must be manually created for disaster recovery. This process is similar to the Ad-Hoc method for user accounts. Additionally, a manual recovery process must be used for these applications.

Service Accounts

For some organizations, certain applications must interact during a disaster. Organizations with greater maturity and experience in managing service accounts can use Privileged Access Management disaster recovery planning. For businesses in different circumstances, a documented plan is needed to ensure service accounts are accessible and usable by applications as part of disaster recovery.

Application Access

Logging into an application is only half of the equation. Stakeholders and customers also require application access. Planning access continuity in a disaster depends on existing application access management methods. Use the following table to review application access options and determine the best fit for your organization.

Method	Description	Pros	Cons
Okta Managed Authorization	Provisions access to integrated applications, or those sending groups to applications as part of Single Sign-On	Fast process Timely recovery turnaround	Groups and other access-related attributes must be included in the objects migrated Adds complexity Requires authentication strategy
Directory based Authorization	Utilizes group mechanisms to manage authorizations in directory-integrated applications	High availability in disaster Requires less effort	Requires regular testing to ensure access data is propagated correctly and applications can reach the directory in disaster
Identity Governance Recovery	Employs an Identity Governance & Administration (IGA) system to recover or provision access in a disaster	Resilient due to reliance on IGAs capacity	IGA system must have its own DRP and be available to support recovery
Manual Provisioning	Manually grant application access	Most straightforward Best for small user populations Good for simple access Ensures access levels/ roles are captured and maintained	Slow Labor-intensive Least scalable Documentation for ad-hoc provisioning must be included in the DRP

Privileged Access & Break-Glass

Privileged Access Management (PAM) systems should be included in the disaster recovery plan. These PAM systems may be secret vaults, jumphosts, and break-glass accounts. Many commercial PAM systems have defined strategies for resilience and disaster recovery. Certain items need to be addressed for organizations without commercial enterprise PAM solutions.

Service Account Credentials

After recovering service accounts, a plan for the credentials is necessary. Most current market solutions allow organizations to ensure secret management at a minimum. Even a cost-effective password manager is better than nothing at all. If primary secret storage is unavailable in a disaster, offline secrets storage or rest and configuration plan can be used to keep your credentials safe.

Offline Secrets Storage

While offline secret storage presents risks, some can be mitigated. Both backing up secrets to a secure offline, physical medium and storing them in a safe location improves offline storage security. Safe deposit boxes and data center vaults are both viable options for storage locations. This offline storage ensures organizations are prepared for disaster, potentially bypassing the need to reconfigure all applications. If your user store recovery does not include password hashes (e.g., manual), document a process to reset service account passwords as accounts are recovered, and closely manage access to these credentials in a recovery.

Reset and Configuration Plan

For some organizations, resetting service account credentials is more practical than restoring them. These organizations should include the process for resetting passwords and reconfiguring dependent applications in the Disaster Recovery Plan. The specific reset and reconfiguration methods should be based on specific application needs, available organizational resources, and risk tolerance levels.

Administrator Access

Disaster Recovery Plans often depend on administrator system access permissions to manually address processes during recovery. But, admin access may be unavailable during a disaster. Depending on the current management of administrator access, ensure a plan for quickly granting administrator access is included in the DRP.

Break-Glass Accounts

Given the risk of being locked out of critical systems in a disaster, break-glass accounts can be a significant advantage. These accounts typically have admin-level or super admin-level access and are created locally in the application or system. Most are not associated with a specific person nor used for daily activities. Instead, this account should be used when there are no alternative means to gain access to a system and recover it.

While functional, these accounts can present their own risks. Therefore, careful precautions are required to protect break-glass accounts. A practical solution is to store the account credentials in an offline, secure, physical location. To ensure optimal security levels, use account logging, user activity, or a check-out system as tracking methods. Wherever practical, application access and logs should be monitored for unauthorized use of these credentials. This ensures remedial action can be taken when necessary.

Despite the risk, break-glass accounts can be a lifesaver for applications where system and data loss can be catastrophic or even fatal to the business. Proceed cautiously, but don't discount the value break-glass accounts can provide in an emergency.

API Access Management

API-first development and micro services are increasingly popular options for tech companies. While these options present numerous benefits, they can also bring significant challenges to organizations with traditional IT architecture. While the complexity of these services is beyond the scope of this guide, consider these two critical factors:

1. All items mentioned previously in the guide must still be accounted for.
2. In addition to the items already mentioned in this guide, detailed user store data, token and authorization policies, and application trust must be handled as well.

A range of specific attributes may be used as token claims or to validate a policy. Thus, recovering these attributes and policies is critical so the tokens can be minted correctly. Take the time to strategically plan their recovery in the event of a disaster, or critical APIs may be inaccessible.

Application trust also becomes a concern in a disaster for API access or micro services. Using Okta or other providers for API Access Management means the recovery tenant will use varying keys to sign tokens. Tokens may have an alternate issuer, and other vital claims may change with the tenant. Services must trust the recovery system to continue permitting API access.

Maintaining the Backup

When it comes to creating backups, there are two main considerations:

1. How often should data be backed up?
2. Where should the backup be stored?

Frequency of Data Updates

The frequency of backups and data updates will depend on the volume and importance of the data. At a minimum, backups and data update frequency should meet your Recovery Point Objective (RPO). If practical, backups and data update frequency can be more frequent than defined by the RPO. Some platforms may lend themselves to frequent automated backups depending on architecture and technology stack. This can be leveraged to your advantage.

Securing the Data

After determining the frequency of backups, it is time to consider where the backups should be stored. Risk and cost should be the determining factors when deciding the best balance of online and offline backups for your organization.

Online Backup

When storing backups online, minimizing the number of individuals with access to the backup is crucial. The individuals who require access to these backups should be identified and listed in the disaster recovery plan.

Who, when, and how online backups are accessed should be identified as part of the disaster recovery plan. Care should be taken to minimize the number of individuals with access. Encryption should be used for sensitive data. Ensuring encryption keys are appropriately secured is critical, and their recovery should be incorporated into the disaster recovery plan. Keys should be stored in a physically secure location that’s quickly and securely accessible to relevant stakeholders.

Offline Storage

Offline backups are a valuable supplement to online backups. Offline methods may require a longer RTO but can be an excellent supplement to simpler, low-cost online backup methods. The location of the offline storage should have physical access controls and auditable logs of activity. Common options for smaller volume storage include bank vaults or vaults in a physical data center. For large-volume storage, specialized vendors can be utilized.

In addition to picking a secure location for offline backup storage, transportation to and from the storage should be considered. Every transportation step to the storage location should be tracked and auditable to ensure the data is not stolen or lost.

Disaster Training & Exercises

Documenting the Disaster Recovery Plan is just the first step to ensuring a seamless disaster recovery. Ensuring the Disaster Recovery Plan is understood and easily implemented is the next step. Training and exercise can be used to ensure quick and efficient implementation of the Disaster Recovery Plan in the event of a calamity.

Recovery training aims to prepare employees for the steps required during and after a disaster. Effective training ensures business continuity can be maintained with ease. To effectively train for disaster recovery, exercises should simulate various disaster scenarios. This provides employees an opportunity to simulate their response to circumstances. Exercise can also identify any gaps in the Disaster Recovery Plan.

Exercises can take various forms, such as tabletop exercises, discussions of specific scenarios, and determining the possible range of effective responses. They can also be full-scale drills. Routinely running disaster recovery training ensures that personnel can efficiently respond to a disaster and quickly recover.

Conclusion

Disaster immunity can never be taken for granted. No technological resource in an IT infrastructure is inherently equipped to cope with the possibility of its occurrence. A strategic Disaster Recovery Plan integrating Okta as a central access management solution is critical to maintaining business continuity when disaster strikes. Effective disaster recovery planning involves identifying potential risks and developing mitigation strategies. Creating a detailed plan to respond to a disaster is a must, regardless of your organization’s size or complexity.

The first step towards effective disaster recovery involves recognizing the organization’s responsibility to protect mission-critical assets. Identifying the scope of your recovery plan will set the building blocks and foundation for a solid communication plan. This plan can be used to relay critical action and initiatives required in the event of a disaster. The plan should also include the following:

- User account stores
- Recovery of external directories
- Authentication and credential strategies
- Core initiatives of application access
- Privileged and break-glass access
- Back-up and recovery methods

Taking precautions and creating strategic measures are vital to operational agility. Regularly reviewing and updating the plan ensures effectiveness and relevance to changing circumstances. A well-structured and strategized disaster recovery plan equips organizations and individuals to handle even the worst of unexpected disasters. This minimizes the impact and damage of a disaster, ensuring business continuity and operational agility recovered easily.

About acsense

Hailing out of Tel Aviv, Israel, the team at acsense, all former Dell-EMC and Okta veterans, have been exposed to the most challenging IT and security ecosystems in the world. After endless IAM implementation use-cases and extensive experience in handling datacenter disasters, the acsense team decided to solve the inherent vulnerabilities in IAM infrastructure.

We offer a cutting-edge IAM resilience platform that caters to both workforce and customer IAM requirements all in one unified solution. Our platform boasts one-click recovery, continuous data verification, routine testing, and the ability to detect alterations between Points in Time, fortifying the resilience of your IAM system.

acsense is backed by Joule Ventures, Gefen Capital, Fusion and independent industry leaders investors.

acsense

Protection And Recovery For Okta Starts Here

To learn more visit www.acsense.com