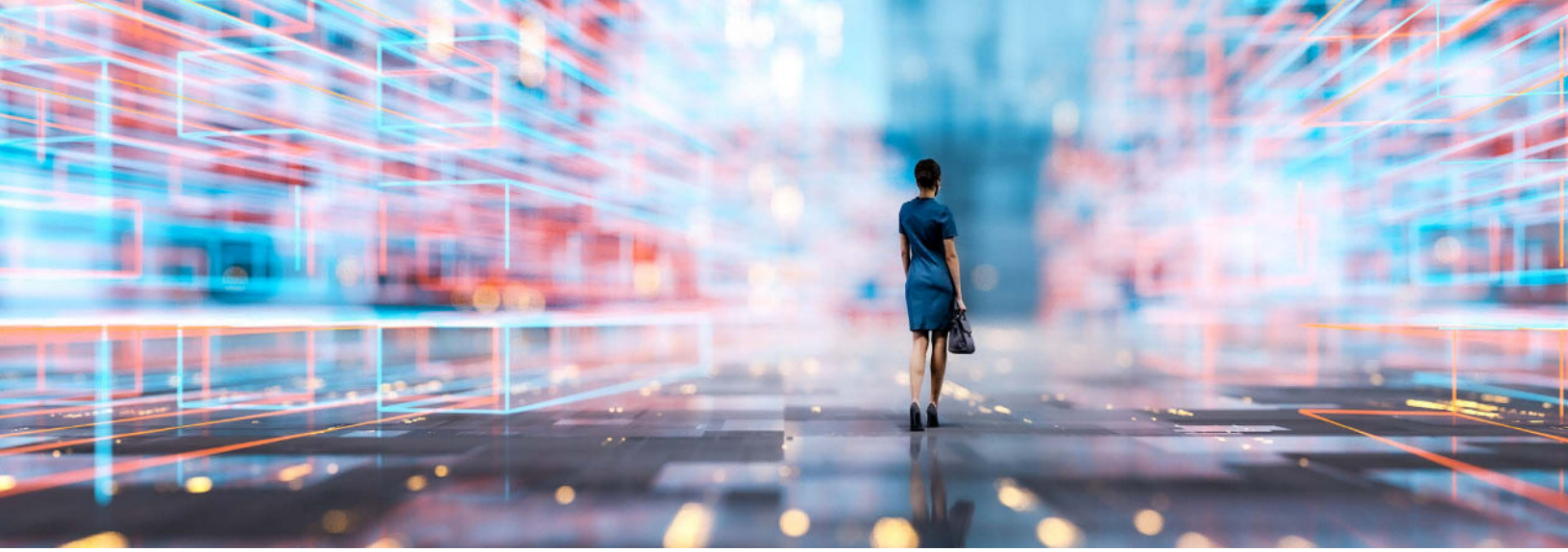
CIO's Guide to

MITIGATING AND REDUCING KEY PERSON DEPENDENCY RISK IN I.T.

DATAPRISE



With the U.S. Department of Labor reporting that 4.4 million Americans quit their jobs in September 2021 and Bankrate discovering that 55% of Americans anticipate looking for new jobs well into 2022, there's no better time for organizations to evaluate their risk of key person dependency.

Key person dependency risk (KPDR) can be a real threat to an organization. This phenomenon occurs when one person exits the company, whether voluntarily or involuntarily, and the gap they leave is so wide that colleagues are truly at a loss about how to move forward. Unfortunately, it's not always apparent just how much control one employee has until they leave. This is especially apparent within IT, as IT leaders and engineers often have institutional knowledge that organizations rely on to "keep the lights on."

The ramifications of KPDR can have long-lasting ripple effects that senior leaders don't always anticipate. The consequences can lead to anything from short-term confusion to long-term reputation damage. For many organizations it can become a business continuity event. Organizations should also be cognizant of insider threat potential when key personnel use their access and knowledge in a manner that could lead to data exfiltration/breach.

Because people often possess the kind of institutional knowledge that takes years to build, reducing key person dependency is often more complex than most people might initially believe. However, there are multiple strategies to help mitigate this type of risk, from cross-training or outsourcing specific roles, to setting up internal systems to catalog institutional knowledge.

To shift from a reactive to a proactive risk management approach, a first step is for organizations to self-evaluate using questions such as the following:

- What exactly occurs when a key person is out of the office? Is it normal for critical tasks to be delayed until they return?
- What are the HR costs involved in hiring and retaining a key position? What are these costs when turnover occurs and someone needs to be hired through an expedited process so as to not incur business operational issues?
- What is the knowledge transfer protocol for when a person leaves the company and how easy is it to follow? Is all the information updated and clear to whomever takes over?

DATAPRISE

- What is the protocol to monitor for and mitigate a hostile ex-employee? Will access systematically be up dated upon departure?
- Are there any individuals that could be considered a single point of failure for the business?

These questions are designed to help organizations understand more about the information, skills, and experience needed should there be a sudden loss of a key person. From license management to updates to network testing, IT personnel are often in charge of tasks that no one else knows how to do. These also typically include background processes such as cybersecurity monitoring and access control.

Below, Dataprise outlines multiple strategies that an organization can use to help minimize this risk, especially in light of the "Great Resignation".

---

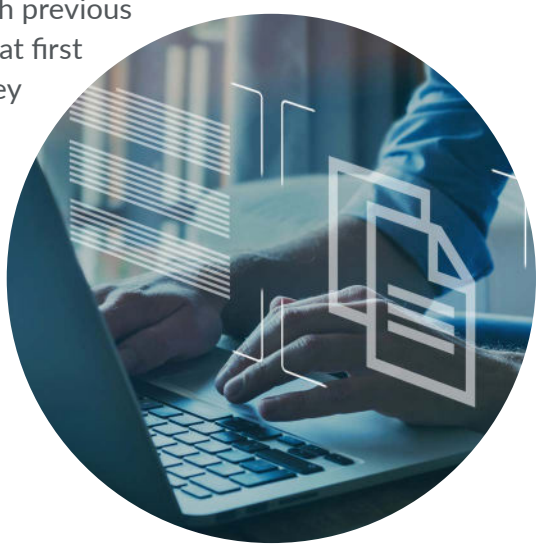
4 Components of a High-Level Strategy

Reducing KPDR at a high level starts with documenting information, establishing configuration management, cross-training or potentially outsourcing specific roles and detailing contingency plans to include human capital management and succession planning.

Developing a Knowledgebase

It's common for organizations to spread critical information over Slack, Google Docs, and email. Employees ask questions over these channels because they know they'd spend far more time trying to find it themselves. Yet all too often that information gets lost and is not easy to search for once a key person departs. Knowledgebases can take many forms, from a standard spreadsheet or database to an intranet site or a wiki page. However a company chooses to do it, the right resource can act as a buoy in the wake of an emergency departure.

This practice is becoming more common today, so staff members don't have to spend time puzzling through scenarios that have already been solved. Instead of performing trial-and-error until they come to the same conclusions, they can simply check an internal knowledge library or consult a configuration management database (CMDB). These articles, containing knowledge gained through previous trial-and-error, are often called "knowledgebase articles," and are a great first step in documenting institutional knowledge that may be lost with a key person departure.



It should be noted that these databases don't have to be set up solely for the IT department either. Some companies will use these same tools to store anything from HR policies to Salesforce configurations to industry contacts.

Tips to create an internal database:

- Include templates, checklists, processes, procedures, and business practice requirements.
- Define how the database will fit with the current knowledge management strategy and which issues it will solve.
- Determine which categories are most important before configuring the central hub.
- Designate people to contribute, edit, and manage the knowledgebase. Allocate duties as necessary to keep people in the loop without endangering security.
- Host a video training where trainers can show employees how to use an internal knowledgebase. Document and evaluate employees' questions and concerns.

The idea is that, regardless of which platform an organization uses, its employees are keeping a consistent formatting and updating structure. Ensuring that the knowledgebase is easy to navigate and access is essential for the success of the initiative. As teams scramble to account for a departed employee, accessible content becomes essential to the continuation of the team's workflow.

This may mean immediately addressing the most important points or answering FAQs in colloquial language rather than technical jargon. As companies develop this database, leaders need to account for how employees are interacting with the tools to gauge the effectiveness of the knowledgebase.

The top criteria for this include:

- **Speed:** Can employees find what they're looking for quickly? Does the search engine need only a few words to accurately determine what the employee is looking for?
- **User experience:** A well-organized database is not only uncluttered, but also easy to adjust when necessary. Anything from adding graphics to creating an article should be intuitive. Team members should also be able to collaborate with one another via the knowledgebase through internal commenting features.
- **Security:** Restrictions within an internal knowledgebase can go a long way to protect information and reduce the odds of both intentional and unintentional breaches. Ensure access is only given to authorized parties.
- **Organization:** Categories should be specific and focused. Subsections should logically flow from each main point. Every word and graphic should provide clear value to the reader on a fundamental level.

The software for knowledgebases has come a long way over the years, and the advancements have helped countless companies record information in a way that benefits everyone. While these sites require skill, time, and effort to put together and maintain, they usually include tools that track how users use the knowledgebase which can be leveraged to enhance the user experience.

Systemization and Documentation

Knowledgebases depend on the systemization and documentation of information. This high-level component goes hand-in-hand with an organization's Business Impact Analysis (BIA), which should absolutely be used as part of an organization's rediscovery roadmap. BIAs not only tell organizations which activities are central to avoiding disruption, they also specify disruption risks and recovery objectives. The ability to find and act upon information will have a lot to do with how fast recovery can get underway.

Systemizing existing processes and evaluating how critical information is shared should be an ongoing process. At Dataprise, we recommend a configuration management database (CMDB) which is used to store asset information throughout their lifecycle and document their interrelationships. Unlike intranet sites that can be applied to anything, a CMDB is typically under the purview of the IT department. Personnel can use it to track the history, connections, and dependencies of anything from facilities to systems to hardware.

Configuration management takes a deeper dive into each asset and defines the health, patterns, and costs of individual elements. A CMDB must include seamless dashboards that show the necessary analytics of what it really means to build and maintain different assets. IT personnel should be able to look at the database and see ongoing trends across assets. If a key person leaves, anyone reviewing the CMDB should feel confident that the information is current and relevant to the organization's operations.

Tips to create a CMDB:

- **Build data models:** A data model will show how configuration relationships should be traced. Some organizations will focus on surface-level connections between critical services and the corresponding infrastructure (e.g., server X to switch Y to router Z). Others will go so far as to show the exact workstations affected.
- **Define types of configuration items (CI):** From hardware and software to documents and people, organizations need to list all configuration items based on the data models chosen. Again, a more basic model may mean selecting critical infrastructure only.
- **Assign owners:** Every CI type should have an owner who will keep track of what information needs to be updated and how the information will be gathered.
- **List attributes:** Attributes like location, version number, and name tell employees more about whether they're working with the right item. Every CI should have these features recorded in the CMDB, and the task should be completed by the individual owner of the CI type.
- **Identify sources:** This step essentially tells people where to find useful information about the CI type. This could include anything from invoices to warranty documentation to serial numbers.
- **Map relationships:** A CMDB is built on the principle of context. This is the big picture rather than a silo of different IT items. The CMDB should be able to, at a high level, show the existing relationships between all the configuration items. This "IT map" should be easy enough to read using the existing data model and can provide an overview to senior leadership on their IT environment overall.

CMDBs are complex and they can be difficult to implement, which is why companies may want to start with isolated or non-critical systems first. For instance, starting with one category (e.g., servers) and verifying the information before moving onto a related category. When testing out the information, it helps to consider how different scenarios might play out.

For instance, if an infrastructure manager wasn't picking up the phone at 3 a.m., how easy would it be to reboot the main routers? Just one mistake in mapping the relationships can wreak havoc, particularly in the face of an unexpected outage or malfunction, so it pays to keep this information straight and up to date.

Cross-Training and Outsourcing

This strategy emphasizes the importance of giving more people insight into the processes of the organization. Rather than directing people to absorb all the information in an internal knowledgebase during a crisis, this high-level tip ensures people are familiar with the information long before they actively need to use it.

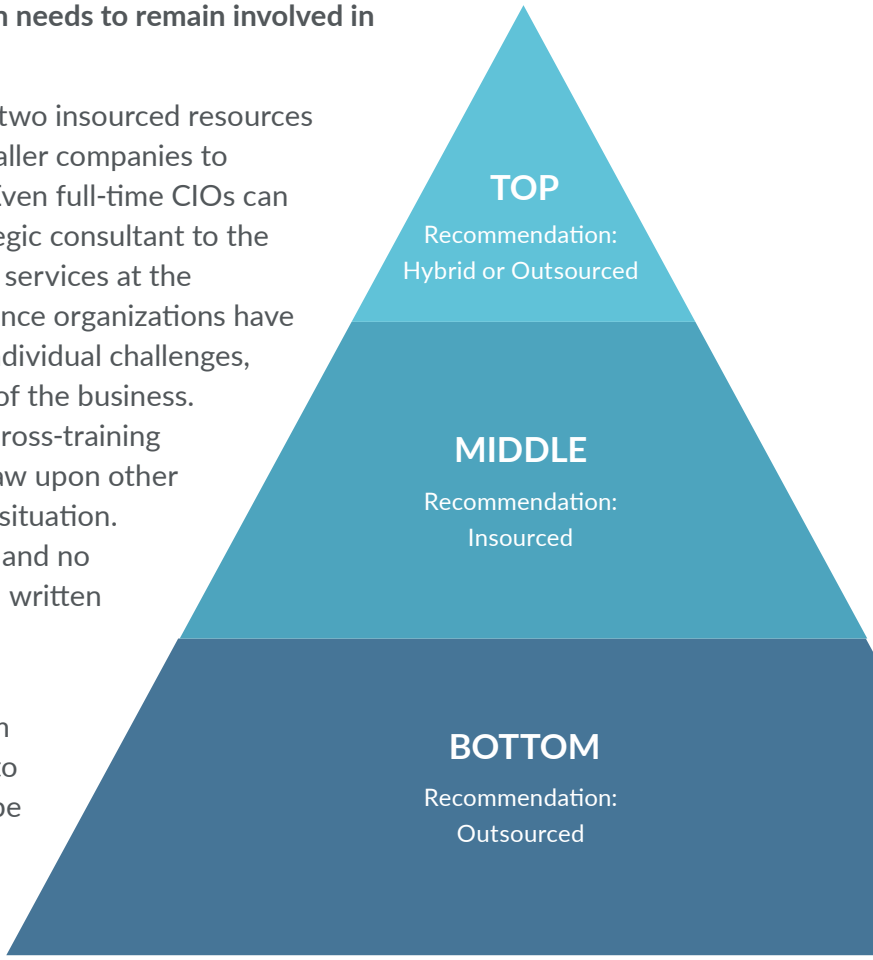
Cross-training can also be an effective way to reduce KPDR while improving employee satisfaction at the same time. These programs have proved lifesaving for companies, particularly when it comes to avoiding workflow interruptions. We recommend starting with clear-cut, measurable goals for your cross-training program before designing and implementing the steps.

Here are the top priorities to keep in mind when devising a cross-training program:

- **Focus on the opportunity:** Quality employees are always looking to expand their repertoire. The more they learn, the more valuable they are to the company and the more leverage they have in their career. This doesn't necessarily have to come with hints of advancement, but a training program should highlight the hidden opportunity for taking on additional responsibilities or learning new skills from their colleagues.
- **Use a training checklist:** Showing the progress of employees makes it easier to see how people are learning. Checklists also make it possible to define realistic timeframes for completion. (This can be exceptionally helpful even for those unexpected personal days a key person might take. Those who are at least partially trained will be able to jump in faster than someone without minimal or no training at all.)
- **Prioritize experience:** Trainers need to be able to both explain what they do and have the experience to give context to each task. It's not always easy to find someone who has both the technical expertise and patience to work with other people, but it is critical for a cross-training program. This disconnect can be a major reason why companies choose to outsource in the first place.
- **Standardize evaluations:** Certification tests are a relatively straightforward way for team members to prove just how much they absorbed during training. It can also reveal to anyone from trainers to CEOs how capable an employee is of manipulating the information to solve real-world challenges. These tests can be completed after each training session as an incremental way to track progress.
- **Talk to employees:** Employees typically have very valuable feedback when it comes to cross-training, particularly if you're seeing the same stumbling blocks across the board. For instance, if multiple employees in the cross-training program have negative feedback about a particular process or workflow, or a negative experience involving an IT system, this is an opportunity for IT or HR to intervene and address the underlying issue that may not have surfaced otherwise.
- **Match employees to their goals:** Ideally in a cross-training program, an organization will factor in not just a person's specialties, but also their interests and long-term career goals. This helps direct the most qualified and motivated people into the right fields for the best results.

There are a lot of moving parts when it comes to cross-training programs, which is why supplementing with outsourcing can be so beneficial. Within IT especially there are three layers to the IT organization. The top layer consists of your strategic senior leaders responsible for staying on the pulse of what drives their organization forward. Next, your middle managers are responsible for managing the expectations from the top, maintaining operations and projects, and delegating to the bottom. The bottom layer includes your engineers, help desk support staff, and technicians dedicated to completing routine tasks. After analyzing countless companies and businesses, we recommend fully or partially outsourcing at the top of the hierarchy, insourcing in the middle, and outsourcing again at the bottom.

This pyramid structure can be what an organization needs to remain involved in the technical output without increasing KPDR:



- **Top:** IT departments will generally have one or two insourced resources at the top. It's not uncommon, however, for smaller companies to outsource to an external team or virtual CIO. Even full-time CIOs can benefit immensely from adding a vCIO or strategic consultant to the team. This strategy provides consistent advisor services at the highest level while drastically reducing KPDR since organizations have access to trained individuals familiar with the individual challenges, infrastructure features, and network demands of the business. What's more, these teams have the benefit of cross-training across multiple clients, making it possible to draw upon other scenarios and provide full context to any given situation. Other benefits include minimal switching costs and no institutional knowledge loss since everything is written down internally.
- **Middle:** As IT operations include recurring maintenance and technical projects, the IT team typically requires one or more roles dedicated to managing this while understanding the full scope of any internally-developed applications or proprietary company knowledge. Therefore, positions like infrastructure and IT operations managers are better off insourced. These are the professionals who understand the goals of the company at both the upper and lower end of the spectrum. Organizations can rely on people in the middle to manage expectations at the top and flesh out the roles at the bottom.
- **Bottom:** Engineers, help desk staff, and technicians typically perform routine tasks that can be completed by a reputable outsourcing team. The best part is that this kind of support can be available 24/7 with the right company, reducing panic when errors or outages occur in the small hours of the morning or over holidays.

Companies like Dataprise were built to free up internal resources. Instead of your best personnel working on low-level tickets, they have the time and energy to devote to more serious matters that have a much larger impact on the profitability of the company, like, for instance, a network that crashes whenactivity exceeds a certain threshold or programs that continually malfunction for customers.

When employees have the opportunity to shine by challenging their own problem-solving skills, it's inevitable that morale will increase and turnover will decrease. When they're constantly disrupted by service requests that stem from outdated infrastructure or poorly trained colleagues, they will find another company that can better appreciate their talents.

Succession and Contingency Plans

Succession and contingency plans are directly related to the efficacy of a disaster recovery plan. When people discuss the latter concept, they often refer to cloud backups and machinery duplications. Yet disaster recovery is more than just backing up your data or automating application failover.

A real recovery plan also includes contingency planning should an organization lose a key member, which will ultimately mean empowering another party to carry out tasks that were once left to a senior professional in the company. This can be a daunting proposition for leaders, which partially explains why KPDR is so common. However, leaving functionality in the hands of just one person creates a single point of failure and should be addressed to avoid a potential business continuity event.

Contingency and succession plans are directly related to cross-training and should include the following stages:

1. **Identify critical positions:** Organizations need to name which positions will be most difficult to fill. This should include roles in which if their authority or control were abused, it could lead to detrimental effects on the goals and health and safety of the organization any components that would be detrimental to the long-term goals, safety, and health of the organization. For instance, if the CIO was let go and still able to retain their access to important documents.
2. **Identify capabilities:** This includes the knowledge and competencies needed to perform tasks that impact business goals. Keep employees informed during this process and use scalable metrics to highlight and control for any gaps. For instance, give a certification test to better evaluate how well a team member knows a programming language that they use sparingly.
3. **Identify interested employees:** Single out professionals who have both the ability to learn critical tasks and the desire to do so. This step should include a discussion of long-term career goals so employees understand how their efforts will be rewarded. For instance, ask a Help Desk technician to learn lower-level tasks from the engineers above them so they can grow into a more advanced role.
4. **Develop and implement a succession plan:** This stage involves both training people on how they can pass on their knowledge and better defining what that information should be. For instance, stepping into a leadership role may be as much about demonstrating empathy to staff as it is about delegating work. From learning to development, the succession plan should give people clear instructions of what is expected from them.
5. **Monitor effectiveness:** Succession plans need to be well thought out if they're going to play a meaningful role during a transition period. Organizations need to consistently evaluate whether their plans allow employees to step into new roles with minimal disruption to the normal workflow.

These steps should be tied into Business Continuity and Disaster Recovery planning. This will not only define how a business will run in an emergency, but also what it means to restore the business to its full functionality. When applied to KPDR, business continuity can be implemented immediately after, for example, a key person leaves for three months on emergency family leave. Disaster recovery can be implemented as soon as the employees designated to fill the position feel comfortable in their new routines. The better the contingency plans, the faster disaster recovery can take over.

This component is heavily dependent on knowing the most important risks to operations so obligations can continue to be met as best as possible. It typically requires testing to ensure employees are both ready and able to keep everything moving. To this end, an organization should consider the development of a risk management program that incorporates KPDR as one of its critical risks.

The Reality of KPDR

Reducing KPDR compels an organization to acknowledge how the loss of a specific team member would affect productivity. Should this event actually occur, there needs to be a comprehensive contingency plan that can be enacted to keep everything up and running.

This is where organizations like Dataprise can prove invaluable to organizations that seek to mitigate and/or address this risk without requiring substantial resources. Our professionals, such as our vCIOs, are uniquely trained to not only advise clients of the best practices for KPDR, but also assist organizations in the development of these initiatives.

vCIOs have flourished in the marketplace because they typically reduce operating costs, focus on leveraging technology to increase revenue, boost productivity, and provide the kinds of analyses that internal employees don't always have the perspective to perform. As a supplementary role to the strategic layer in the organization, vCIOs also help address KPDR by providing access to teams of resources with low switching costs should turnover occur. Dataprise vCIOs routinely look for process and operational improvement, cybersecurity vulnerabilities, compliance gaps, and financial optimization opportunities and present these in roadmaps and action plans to senior leadership. As organizations seek to reduce their KPDR, leveraging MSPs like Dataprise is a sure-fire way to address what keeps leadership up at night: Can my organization withstand a disaster event? Will my organization continue to operate efficiently if we lose our key personnel?

At Dataprise, we have the solutions available to assist with all the strategies listed above and help your organization reduce key person dependency risk. Learn more about our Strategic IT Infrastructure and Cybersecurity services and Business Continuity and Disaster Recovery services on our website.

About Dataprise

Founded in 1995, Dataprise is the leading strategic IT solution provider to midmarket IT leaders who believe technology should allow you to be the best at what you do. Dataprise's unbeatable IT solutions and services are tailored to the needs of strategic CIOs and provide best-in-class managed security, network, infrastructure, collaboration, and end-user solutions. Dataprise has offices across the United States to support our clients.

LET'S TALK!

1.888.519.8111
www.dataprise.com