CALIFORNIA JUDICIAL BRANCH

Disaster Recovery Framework

A Recommendations & Reference Guide for the California Judicial Branch

VERSION 2.3

OCTOBER 22, 2017

JUDICIAL COUNCIL OF CALIFORNIA
INFORMATION TECHNOLOGY ADVISORY COMMITTEE

Table of Contents

1.0 INTRODUCTION

The Judicial Branch Disaster Recovery Framework serves as a model and aid for implementing and maintaining a lean and robust information technology (IT) disaster recovery (DR) solution. The framework and related reference materials will assist judicial branch entities (JBEs) with establishing a disaster recovery strategy and will offer recommendations and examples of products and services that can accommodate the varying needs of small to large Supreme, appellate, and superior courts. The Supreme Court, the Courts of Appeal, and the superior courts (hereafter collectively referred to as JBEs) are not required to implement the framework in its entirety; rather, the intent is to highly encourage JBEs to use the framework as a template to develop a disaster recovery strategy and solution most appropriate to their unique local business requirements. Additionally, each court's disaster recovery implementation will differ significantly based on factors such as geographic location, natural disaster risk ratings, types of hosting solutions in use, and varying business drivers. The framework is for use as a guide and versatile benchmark of what should be in place in each JBE.

This guide is intended to provide a roadmap for JBE's and does not include all the details or steps required for implementing a trusted, fail-safe disaster recovery plan or solution. It does, however, provide tools and examples for JBEs to design disaster recovery solutions appropriate to their needs and recommend ways to ensure the integrity and usefulness of the those solutions.

2.0 DEFINITION

A disaster recovery plan includes a set of branch policies, procedures, diagrams, documentation, systems, and tools "to enable the recovery or continuation of vital technology infrastructure and systems following a *natural* or *human-induced disaster*."[1] It also includes a robust redundant and/or alternate infrastructure to facilitate quick recovery of critical systems, with regular defined intervals of testing that occur to ensure the integrity of the approach.

3.0 PURPOSE OF DISASTER RECOVERY

Data and electronic information are paramount to the operation and success of each judicial branch entity. The broad term *information system* is used to identify a human and electronic process for the collection, organization, storage, and presentation of information. Consistent with that of other industries, JBEs' use of systems and technology has increased over time. Any JBE would be challenged to continue normal operations without systems that have become integral to business process.

[1] Wikipedia contributors, "Disaster recovery," *Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Disaster_recovery&oldid=772607446* (as of May 9, 2017), referencing Georgetown University, Business Continuity and Disaster Recovery, *Disaster Recovery, https://continuity.georgetown.edu/dr* (as of May 9, 2017).

The purpose of IT disaster recovery is to restore or maintain operations of technology systems supporting critical business functions following a natural or human-induced disaster. Although this document focuses primarily on IT disaster recovery, it is important that the disaster recovery plan support and align with the business continuity plan and/or other established plans and protocols that JBEs have in place (e.g., Continuity of Operations Plan, *https://coop.courts.ca.gov*).

Consideration should also be given to aligning the JBE disaster recovery plan to those of applicable justice partner agencies. The goal is to facilitate restoration of related or dependent services across agencies where possible.

Technologies such as backup, off-site storage, replication, and private/hybrid cloud, and metrics such as recovery point objective (RPO) and recovery time objective (RTO) are all valid discussion points and planning considerations when reviewing disaster recovery options.

A disaster recovery plan should be tailored to the individual JBE, with the goal that vital systems are preserved and made operational at performance, availability, and cost levels that meet JBE business continuity objectives.

4.0 DISASTER RECOVERY FRAMEWORK

4.1 Scope

The disaster recovery framework has been developed for the establishment of a baseline reference model for disaster recovery within the judicial branch of California. It is known that existing and future DR plans put into place by JBEs will differ from one another primarily because of varying logistics and challenges with facilities, geographic locations, funding, and/or internal requirements. To produce the framework, input was solicited from multiple courts ranging in size from small to large so that a comprehensive framework could be developed that suits all entities within the judicial branch. The framework is designed to set a direction, identify and address the growing importance of DR within the branch, and ensure that the rapid evolution and adoption of technology within the branch are complemented with a plan to ensure the integrity of electronic data and systems.

The goals of the framework are to:

- Encourage a JBE to assess their current environment and conduct a DR maturity analysis;
- Suggest and define model disaster recovery guidelines for the branch;
- Suggest and define standard recovery times and priorities for each of the major technology components of the branch;

- Be usable by all judicial branch entities as a court's disaster recovery plan;
- Provide baseline guidance for backups and high-availability options and scenarios for JBEs to incorporate into their disaster recovery strategies;
- Provide visual reference of various disaster recovery scenarios;
- Provide guidance to all members of the judicial branch on establishing methods of applying disaster recovery and therefore ensuring the integrity, survivability, and recoverability of various systems and data; and
- For each platform, operating system, application, and security device, provide the basis for the development of implementation standards, procedures, and guidelines that can then be monitored and enforced against the recommendations defined in the framework.

4.2 Organizational Characteristics

The framework establishes how various systems and data are to be backed up and protected from data loss and will be made highly available to mitigate the chances that the disaster recovery plan would need to be relied on. Some judicial branch entities interface and share data with one another, increasing the complexities and risk factors of data ownership and protection. Additionally, because of the complex inner workings of the judicial branch and each individual JBE, each court's Continuity of Operations Plan (COOP) overlaps. The IT DR plan and all related material should be placed into and support the COOP. It is not, however, a replacement for the COOP, and neither is the COOP a holistic solution for IT disaster recovery.

4.3 Organizational History and Importance of Disaster Recovery

Over the past decade, JBEs have increasingly deployed more and more technology to increase operational efficiencies, improve public access to justice, and to streamline interaction with various justice partners. Specifically, over the last four years, as a result of budget reductions and other hardships, some JBEs have elected and others were forced to deploy and host their own case management systems: systems that were once managed by a central entity or provider (e.g., the judicial branch, with its California Courts Technology Center [CCTC] or a respective county). Additionally, some JBEs have begun using cloud-provided services, systems, and software, drastically changing the traditional approach to disaster recovery and how data is backed up and preserved.

4.4 Supporting References and Content

Following are some sources and publications that the Judicial Council's Information Technology Advisory Committee (ITAC) referenced in the development of this framework:

- Next Generation Hosting Strategy Workstream output(s) (ITAC deliverable pending)
- Information Systems Controls Framework (Judicial Council and ITAC deliverable)
- California Courts Technology Center
- NASCIO—*Cyber Disruption Response Planning Guide* (*www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf*)
- National Institute of Standards and Technology—Special Publication 800-34 Rev. 1 (Contingency Planning Guide for Federal Information Systems) (*http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf*)

4.5 Documentation Structure

An IT disaster recovery plan is supported by documentation that captures differing levels of detail while ensuring that the plan is flexible enough to adapt as organizational and IT priorities and dependencies change. The IT disaster recovery framework should consist of the following categories of documents:

- Organizational policy (for JBEs)—expresses management's expectations regarding disaster recovery and importance of data, including expectations for time to recover based on categorized tiers of data types and importance.
- IT department policy—further refines management's expectations, specifically of data protection from a technical perspective and for safeguarding electronic data from loss or destruction within specified parameters, as defined by the local entity. The department policy informs IT staff of the department's comprehensive approach toward disaster recovery, ensuring that all subdivisions in the department are working cohesively to comply.
- List of systems/data categorized by recovery time—a complete categorized list of data assets broken into tiers of criticality, including specific hardware, systems, software, and data that support the mission of the JBE. This document includes the ITAC-recommended criticality ranking of many systems; however, local organizational policy within each JBE may necessitate changes to the list.
- List of appendixes
    - Appendix A: List of high-level technical requirements and systems and data categorized by recovery time
    - Appendix B: Recommended minimum requirements for a backup solution

- List of types of events that would trigger the declaration of a disaster or operational crisis to the JBE/region
    - Loss of data center (natural, by fire, by water, etc.)
    - Infrastructure or major equipment failure
    - Power outage or significant voltage surge
    - Cloud-hosted–circuit outage (single point of failure) or cloud data center outage (single point of failure)
    - Severing of communication cables (cut fiber, etc.)
    - Security breach
    - Data hostage situation (e.g., ransomware)
    - Malicious behavior—internal sabotage
    - Malicious behavior—vendor sabotage

- Checklists
    - Planning
    - Implementation and milestones
    - Verification and testing

- Guidelines—recommendations that can be used when other guidance has not been established. Guidelines are usually created at lower operational levels, such as by departments, to address immediate needs until consensus is reached on broader direction.

5.0 SUPPORTED AND RECOMMENDED BACKUP TECHNOLOGIES

5.1 Disk

A disk is a data storage device used for storing and retrieving digital information. It is a type of nonvolatile memory, retaining stored data even when powered off.[2]

- Pros
    - **Local**. Data is on the premises and therefore within your control.
    - **Speed**. Because data is local, it is typically accessed from internal networks that are capable of providing faster access times. There is also no overhead from latent internet bandwidth.
    - **Security**. Disks are not managed by a third party, which can protect your data from hacking and loss of privacy.

- Cons
    - **Management**. Controlling access to data—including virus protection and vulnerability protection—becomes the responsibility of the local agency.

[2] Wikipedia contributors, "Cloud computing," *Wikipedia, The Free Encyclopedia,* *https://en.wikipedia.org/wiki/Hard_disk_drive* (as of May 30, 2017).

- **Cost**. Disks require upfront capital expense in addition to ongoing maintenance contracts when used in mission-critical applications.
- **Physical security**. Protection from physical threats including fire, water damage, and natural disaster are paramount and become the responsibility of the local agency.

5.2 Cloud

"Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand."[3]

- Pros
  - **Cost**. Onsite hardware and capital expenses are unnecessary and storage costs relatively low because you pay only for the storage you require.
  - **Expansion**. Scalable architecture allows for convenient provisioning of additional storage space as needed.
  - **Offsite location**. Data can be stored in geographically distinct locations, possibly preventing loss from disaster.
  - **Physical security**. Leading cloud providers typically take on the responsibility of keeping your data highly secure and mirrored across multiple centers within the United States. *Note: When using a cloud vendor, care should be taken to ensure all of a JBE's data, including all replicas are housed and maintained within the United States. Additionally, it is important to clearly analyze and understand what level(s) of data protection and recovery options the cloud provider includes or offers.*

- Cons
  - **Outages**. If the Internet goes down on your side or on your cloud provider's side, you may lose access to your information until the issue is remediated.
  - **Bandwidth**. Large amounts of bandwidth are required to conduct data/storage transfers and a lack of sufficient bandwidth can lead to performance degregations
  - **Exclusivity**. Once data has been transferred and procedures have been implemented, moving data/storage to another provider may be challenging.
  - **Privacy and security**. With private data exposure and data hostage situations becoming more commonplace, the cloud poses newer and varying security risks, some of which are still unknown. Careful analysis and IT controls should be framed around managing permissions (both internal and external), confidentiality of intellectual property, accidental and intentional deletion on individual, shared and cloud drives and clear-cut audit trails.
  - **Complexity.** Cloud technology can present newer and unknown challenges in regards to control and troubleshooting. All interaction with cloud computing is through the use of technology and the ability to remediate issues is limited to the response time of the supporting systems and hosting provider(s)' call centers.

[3] Wikipedia contributors, "Cloud computing," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/wiki/Cloud_computing (as of May 30, 2017).

NOTE: Tape technology is not a current or recommended backup medium for production and/or critical data. However, in certain circumstances where there may be a lack of bandwidth and options to increase bandwidth are limited or considerably expensive, tape may be an appropriate backup medium. Tape may also be a feasible choice for lab/test environments.

6.0 CONTINGENCY STRATEGIES

Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the business impact analysis. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

The selected recovery strategy should address the potential impacts identified in the business impact analysis and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice will depend on the incident, type of system and operational requirements. Specific recovery methods should be considered and may include commercial contracts with cold, warm, or hot backup-site vendors (see section 6.3); cloud providers; mirrored sites (see section 6.3.4); reciprocal agreements with internal or external organizations; and service-level agreements (SLAs) with the equipment vendors. In addition, technologies such as RAID (redundant array of independent disks), automatic failover, uninterruptible power supplies, and mirrored systems should be considered when developing a system recovery strategy.

6.1 Backup Methods

System data should be backed up regularly. Policies should specify the frequency of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. Data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. Data may be backed up on magnetic disks, cloud storage or other common-day and reliable mediums. The specific method for conducting backups should be chosen based on system and data availability and integrity requirements. Methods include electronic vaulting, storing to mirrored disks (using direct-access storage devices [DASDs] or RAID), and storing to cloud provided storage platforms.

Storing backed-up data offsite is *essential* business practice. Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. With offsite storage, data is backed up at the organization's facility and then labeled, packed, and transported to the storage facility. If the data were required—for recovery or

testing, for example—the organization would contact the storage facility and request specific data/disks to be transported to the organization or to an alternate facility. Commercial storage facilities often offer media transportation and response and recovery services.

When selecting an offsite storage facility and vendor, the following criteria should be considered:

- Geographic area—distance from the organization and the probability of the storage site's being affected by the same disaster that might strike the organization
- Accessibility—length of time necessary to retrieve the data from storage, and the storage facility's operating hours
- Security—security capabilities of the storage facility and employee confidentiality, which must meet the data's sensitivity and security requirements
- Environment—structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls)
- Cost—cost of shipping, operational fees, and disaster response and/or recovery services

6.2 Alternate Sites

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, the plan must include a strategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

- Dedicated site owned or operated by the organization
- Reciprocal agreement or memorandum of agreement with an internal or external entity
- Commercially leased facility
- Cloud

Regardless of the type of alternate site chosen, the selection must be able to support system operations as defined in the contingency plan. Thetypes of alternate sites may be categorized in terms of their operational readiness. Based on this factor, sites may be identified as cold, warm, hot, mobile, or mirrored sites. Progressing from basic to advanced, the sites are described below.

6.3 Recovery Options

6.3.1 Cold site

A cold site typically consists of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system. The space may have raised floors and other attributes suited for IT operations. The site does not contain IT equipment and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities.

6.3.2 Warm site

Warm sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. A warm site is maintained in an operational status ready to receive the relocated system. The site may need to be prepared before receiving the system and recovery personnel. In many cases, a warm site may serve as a normal operational facility for another system or function, and in the event of contingency plan activation, the normal activities are displaced temporarily to accommodate the disrupted system.

6.3.3 Hot site

Hot sites are office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, seven days a week. Hot-site personnel begin to prepare for the system arrival as soon as they are notified that the contingency plan has been activated.

6.3.4 Mirrored site

Mirrored sites are fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data are processed and stored at the primary and alternate sites simultaneously. These sites typically are designed, built, operated, and maintained by the organization.

6.3.5 Cloud

A cloud “location” can serve as warm, hot, or mirrored site and have a number of other benefits and purposes. Cloud offerings can provide remote and virtual infrastructure and are typically rated at a high-tiered classification for uptime, reliability, and scalability. Contracted services are often available through cloud

providers to help with a JBE's disaster recovery strategy and goals that require technical assistance by the cloud provider. For additional offerings and recommendations relative to the cloud, please reference the judicial branch Next Generation Hosting Strategy Workstream deliverables.

6.4 Selecting an Option

The cost and ready-time differences among the four options are obvious. The mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain; however, they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) that affected the organization's primary site. The table below summarizes the criteria that can be employed to determine which type of alternate site meets the organization's requirements. Sites should be analyzed to ensure that the security, management, and operational and technical controls of the systems to be recovered are compatible with the prospective site. Such controls may include firewalls and physical access controls, data remanence controls, and security clearance levels of the site and staff supporting the site.

Alternate-Site Selection Criteria

Site	Cost	Hardware Equipment	Telecommunications	Setup Time	Location
Cold	Low	None	None	Long	Fixed
Warm	Medium	Partial	Partial/Full	Medium	Fixed
Hot	Medium/High	Full	Full	Short	Fixed
Mirrored	High	Full	Full	None	Fixed
Cloud	Medium/High	N/A	Mixed	Short	Agile

These alternate sites may be owned and operated by the organization (internal recovery), or commercial sites may be available under contract. Additionally, cloud providers can provide IaaS (Infrastructure as a Service) computing that mimics a colocation site and offers near-unlimited services and opportunities. If contracting for the site with a commercial vendor, adequate testing time, workspace, security requirements, hardware requirements, telecommunications requirements, support services, and recovery days (how long the organization can occupy the space during the recovery period) must be negotiated and clearly stated in the contract. Customers should be aware that multiple organizations may contract with a vendor for the same alternate site; as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor's policy on how this situation will be addressed and how priority status is determined should be negotiated.

Two or more organizations with similar or identical IT configurations and backup technologies may enter into a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. With sites that serve as alternate sites for each other, a reciprocal agreement or memorandum of understanding (MOU) should be established. A reciprocal agreement should be entered into carefully because each site must be able to support not only its own workload but the other organization's as well, in the event of a disaster. This type of agreement requires the recovery sequence for the applications from both organizations to be prioritized from a joint perspective, favorable to both parties. Testing should be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and backup configurations, sufficient telecommunications connections, compatible security measures, and sensitivity of data that might be accessible by other privileged users, in addition to functionality of the recovery strategy.

An MOU, memorandum of agreement (MOA), or a service level agreement (SLA) for an alternate site should be developed specific to the organization's needs and the partner organization's capabilities. The legal department of each party must review and approve the agreement. In general, the agreement should address at a minimum, each of the following elements:

- Disaster declaration (i.e., circumstances constituting a disaster and notification procedures)
- Site and/or facility priority access and/or use
- Site availability
- Site guarantee
- Other clients subscribing to the same resources and site, and the total number of site subscribers, as applicable
- The contract or agreement change or modification process
- Contract or agreement termination conditions
- The process to negotiate extension of service
- Guarantee of compatibility
- IT system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software)
- Change management and notification requirements, including hardware, software, and infrastructure

- Security requirements, including special security needs
- Whether staff support is provided
- Whether facility services are provided (use of onsite office equipment, cafeteria, etc.)
- Testing, including scheduling, availability, test time duration, and additional testing, if required
- Records management (onsite and offsite), including electronic media and hard copies
- Service-level management (performance measures and management of quality of IT services provided)
- Workspace requirements (e.g., chairs, desks, telephone, PCs)
- Supplies provided or required (e.g., office supplies)
- Additional costs not covered elsewhere
- Other contractual issues, as applicable
- Other technical requirements, as applicable

6.5 Equipment Replacement[4]

If the IT system is damaged or destroyed or the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. Three basic strategies exist to prepare for equipment replacement. When selecting the most appropriate strategy, note that the availability of transportation may be limited or temporarily halted in the event of a catastrophic disaster.

6.5.1 Vendor agreements

As the contingency plan is being developed, SLAs with hardware, software, and support vendors may be made for emergency maintenance service. An SLA should specify how quickly the vendor must respond after being notified. The agreement should also give the organization priority status for the shipment of replacement equipment over equipment being purchased for normal operations. SLAs should further discuss what priority status the organization will receive in the event of a catastrophic disaster involving multiple vendor clients. In such cases, organizations with health- and safety-dependent processes will often receive the highest priority for

[4] Section 6.5 is taken from NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010), § 3.4.4, pp. 24–25, *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf* (as of May 10, 2017).

shipment. The details of these negotiations should be documented in the SLA, which should be maintained with the contingency plan.

6.5.2 Equipment inventory

Required equipment may be purchased in advance and stored at a secure off-site location, such as an alternate site where recovery operations will take place (warm or mobile site) or at another location where they will be stored and then shipped to the alternate site. This solution has certain drawbacks, however. An organization must commit financial resources to purchase this equipment in advance, and the equipment could become obsolete or unsuitable for use over time because system technologies and requirements change.

6.5.3 Existing compatible equipment

Equipment currently housed and used by the contracted hot site or by another organization within the agency may be used by the organization. Agreements made with hot sites and reciprocal internal sites stipulate that similar and compatible equipment will be available for contingency use by the organization.

When evaluating the choices, the contingency planning coordinator should consider that purchasing equipment when needed is cost-effective, but can add significant overhead time to recovery while waiting for shipment and setup; conversely, storing unused equipment is costly, but allows recovery operations to begin more quickly. Based on impacts discovered through the business impact analysis, consideration should be given to the possibility of a widespread disaster requiring mass equipment replacement and transportation delays that would extend the recovery period. Regardless of the strategy selected, detailed lists of equipment needs and specifications should be maintained within the contingency plan.

7.0 PROVEN AND AVAILABLE TECHNOLOGIES AND PRODUCTS

7.1 Technologies Currently Deployed in the Branch

The following currently deployed technologies and in use throughout the branch help JBEs meet their disaster recovery plan objectives:

- Barracuda Backup with secondary Barracuda Backup appliance and/or cloud replica(s)
- Barracuda Cloud-to-Cloud Backup
- Barracuda Essentials for Office 365
- VMware Site Recovery Manager

- Various cloud providers
- Various storage area network (SAN) solutions with "snapshot" and "lagged mirror" technology

7.2 Potentially Useful Technologies Not Known to be Implemented in the Branch

Following are examples of technologies that are believed not yet to have been implemented in the branch, but that exhibit strengths in disaster recovery objectives:

- Veeam Backup & Replication with cloud replica
- Rubrik Cloud Data Management with cloud replica
- Amazon Web Services (AWS) Storage Gateway
- Microsoft Azure Site Recovery
- Veeam DRaaS (Veeam Cloud Connect)
- Hyperconverged infrastructure/solutions that can accomplish a JBE's DR initiative(s)

NOTE: The products and/or technologies listed above are for baseline reference purposes only. JBEs do not have to choose one of these solutions, but rather can use the technologies on the list or reference the list to determine what solutions best fit within their technology environments and meet their recovery objectives.

8.0 EXAMPLE SCENARIOS AND DEPLOYMENT SOLUTIONS

Disaster recovery scenarios can be very complex and impossible to work out without specific details. Sections 8.1–8.3 offer guidelines for some general scenarios. Note that a number of caveats to implementation must be taken into account when creating a disaster recovery scenario, including the following:

- **Identify business-critical servers and data**. Identifying the business-critical servers and data will provide the information required to size the disaster recovery scenario. This information is critical to scenarios pertaining to cloud services and physical hardware.
- **Determine data circuit requirements**. Using the information from the identifying server and data needs will allow the JBE to determine the bandwidth requirements to support the replication and synchronization of the DR scenario.

- **Identify technology to facilitate DR**. Identifying the technologies in use is important. DR scenarios are intended to assist in implementing a DR plan for IT and so focus on electronic data. However, JBEs may have critical data that are not in electronic format. Therefore, the JBE needs to identify technologies that can be used to assist in the DR plan. As an example, if a court has gone paperless, it can store the documentation for cases on the cloud, leaving the documentation accessible during an outage or disaster. However, if the court still stores paper case files, in the event of a disaster the court may lose those paper files and be unable to recover them. Another component that can support a JBE's DR strategy is through the use of virtualization technology, which allows for easy transfer of servers between data center and cloud.

- **Identify physical requirements**. Many of the scenarios in section 8.0 require physical hardware and, therefore, the related space, racks, servers, network equipment, and appliances. It is important to identify what equipment will be necessary and to ensure that power and cooling are sufficient to meet the needs of that equipment following a disaster. However unlikely it is, these scenarios may one day be running the critical court operations for a JBE, and they should be provided similar resources to the primary data center.

- **Identify public-relations impact.** Careful thought should be taken into consideration in regards to media and what the news may look like on the front page of a JBE's local newspaper.

- **Identify cost(s) or backlog impact**. A detailed business impact analysis should be conducted to determine what financial and/or labor/backlog impact may result from both short-term and long-term outages. The results of this analysis will help a JBE prioritize recovery objectives and sequencing.

To discuss DR scenarios effectively, a common starting point for the differing terminology is also essential. In many cases, different definitions for the same terminology are floating in the ether. Below are several relevant terms and their definitions:

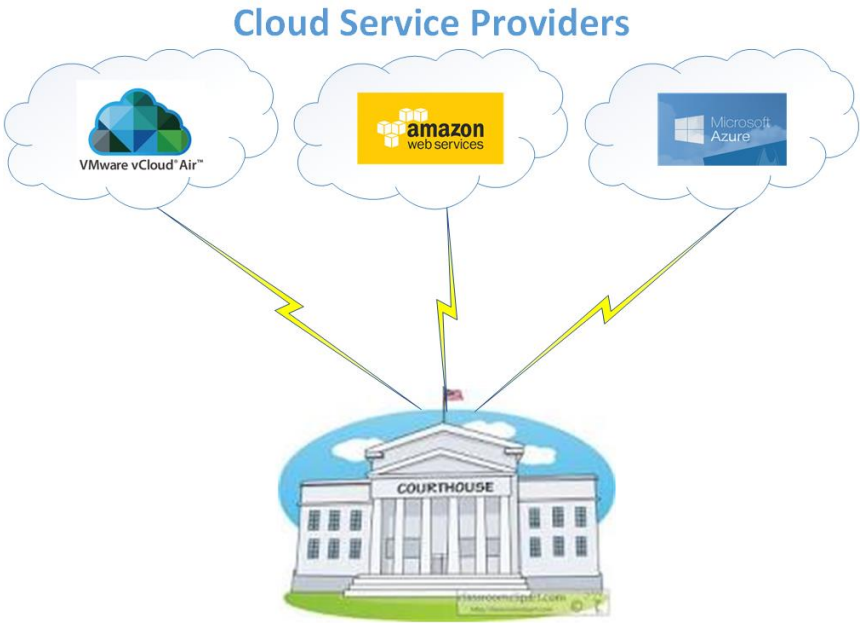
- Public cloud—a network of remote servers and storage hosted by a vendor and accessible on the Internet. It allows for the storage, management, and processing of data offsite, rather than using local resources. Cloud advantages include scalability, instant provisioning, and virtualization of resources. The public cloud typically shares resources among many tenants or customers.

- Private cloud—similar to a public cloud, but resources are dedicated to a single tenant or customer. A private cloud can also reside on the premises, providing the benefits of local use and control while leveraging the benefits of a cloud computing platform. Examples of on-premises private cloud solutions are VMware, Nutanix, and Microsoft Hyper-V hypervisor. On-premises private cloud offers the same advantages as any other cloud, including scalability, instant provisioning, and virtualization.

- Hybrid cloud—a cloud computing environment using a mix of cloud services (public and private) and on-premises hardware (standard data center) to facilitate communication between a data center and cloud services.

- Cloud service providers—vendors who sell public and private cloud services and hybrid solutions. Top-tier cloud service providers include Amazon Web Services, Google, Microsoft, VMware and Oracle. The top-tier providers offer comprehensive solutions for virtually any cloud computing needs with multiple cloud service locations to ensure maximum survivability.

Figure 1: Cloud Service Providers



- Disaster recovery (DR)—a set of policies and procedures to enable recovery of critical technology infrastructure and systems following a major outage or disaster. DR's main goal is to protect data and ensure that business can resume as quickly as possible following an event.

- Business continuity (BC)—the ability to continue to deliver services at a predefined level following an outage or disaster. Whereas DR allows you to protect data and rebuild, BC allows you to continue running through the outage or as soon as possible thereafter depending on the specific events.

- Colocation data center—a third-party data center where rack space can be rented to host physical hardware such as servers and appliances. Colocation data centers have a rating supplied by the Uptime Institute to let you know how much uptime you can expect. The ratings range from Tier I to Tier IV, with the highest tier providing the highest uptime and fault tolerance.
  - Tier I: Minimum of 99.671 percent availability, with no redundancy in power, cooling, or network
  - Tier II: Minimum of 99.741 percent availability; N+1 redundancy in power and cooling

  - Tier III: Minimum of 99.982 percent availability; N+1 redundancy in power, cooling, and network, with multiple uplinks for data
  - Tier IV: Minimum of 99.995 percent availability; 2N+1 redundancy in power, cooling, and network, with multiple uplinks for data

  Examples of Tier III and Tier IV data centers are Recovery Point's Gaithersburg Data Center and Switch's SUPERNAP, respectively.

- Data egress and ingress—data traffic in and out of the cloud. Egress data traffic comes from an external source into the cloud. Think of this as uploading data to the cloud, such as when backing up data to the cloud or synchronizing on-premises servers with servers in the cloud. Ingress data traffic comes from the cloud to on-premises servers. Think of this as the download of data from the cloud, such as in a data recovery from cloud storage or when accessing running servers in the cloud. The terminology is important because vendors charge different amounts per gigabyte depending on whether the data constitutes egress or ingress traffic.

- Load balancers—appliances that manage redundant systems, allowing users to be directed to different servers for the same data. For example, load balancing can be used for a SharePoint intranet site to point the user to one of two redundant SharePoint servers (e.g., Sharepoint1 or Sharepoint2) to balance the number of connections and bandwidth. A load balancer can also be used to point to one application or server primarily and point to a secondary one in the event of an outage.

- Tapeless backup appliance—an appliance designed to replace a tape backup system. Typically, these appliances consist of a large amount of storage to hold backups. The appliance also often has data management tools built in. Various backup appliances also have native support for many top-tier cloud service providers to ensure seamless data replication.

- Warm or hot sites—physical locations for DR and their availability. Warm sites consist of hardware and network connectivity to support production but are not 100 percent up to date, require manual intervention, and can take hours or days to bring online. Hot sites are duplicates of production environments with real-time synchronization; they run concurrently with the main production site. Switching to a hot site can take minutes to bring online.

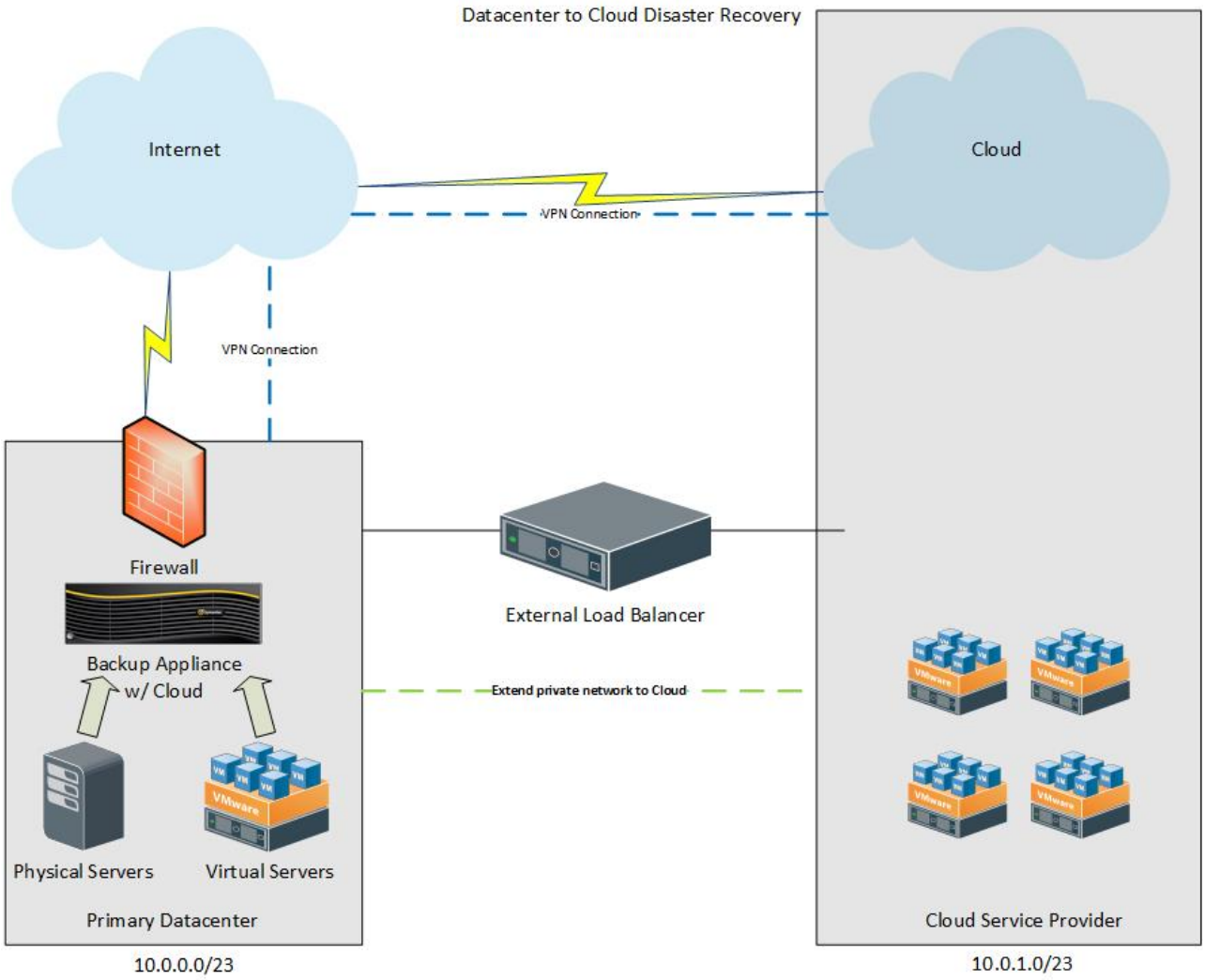
8.1 Single-Site Small or Medium JBE

8.1.1 Scenario 1: Cloud-based DR

Cloud-based **DR** is the preferred **DR/BC** scenario. Depending on business need, the cloud can be used as offsite storage to replace tape backups; as a **public cloud** or **private cloud** for storage, replacing or supplementing the local SAN; or for **business continuity**, encompassing the **public cloud** and **private cloud** and introducing aspects of the **hybrid cloud** to allow virtual servers to be synchronized on the cloud and turned up as needed during outages or disasters. **Cloud service providers** allow

JBEs to replace tape backups, store tapes offsite, and virtualize data stores and critical servers and put them up on the cloud for a monthly fee plus **data ingress and egress**. The data are accessible for daily use, for recovery, or during outages and disasters. Additionally, servers can be switched from standby to active in minutes and reached as long as the Internet is accessible, functioning in the same manner as physical or virtual servers onsite. A dedicated Internet circuit (sized based on data requirements) is required to ensure that data and servers are replicated to cloud services regularly. To simplify management of data on the cloud and facilitate replication and synchronization, several types of **tapeless backup appliances** can be implemented to ensure data integrity in the cloud. And with top-tier **cloud service providers**, the JBE can often extend the internal network to the cloud, in concert with a **load balancer**, which can make failover significantly less painful.

Figure 2. Cloud-Based DR Diagram

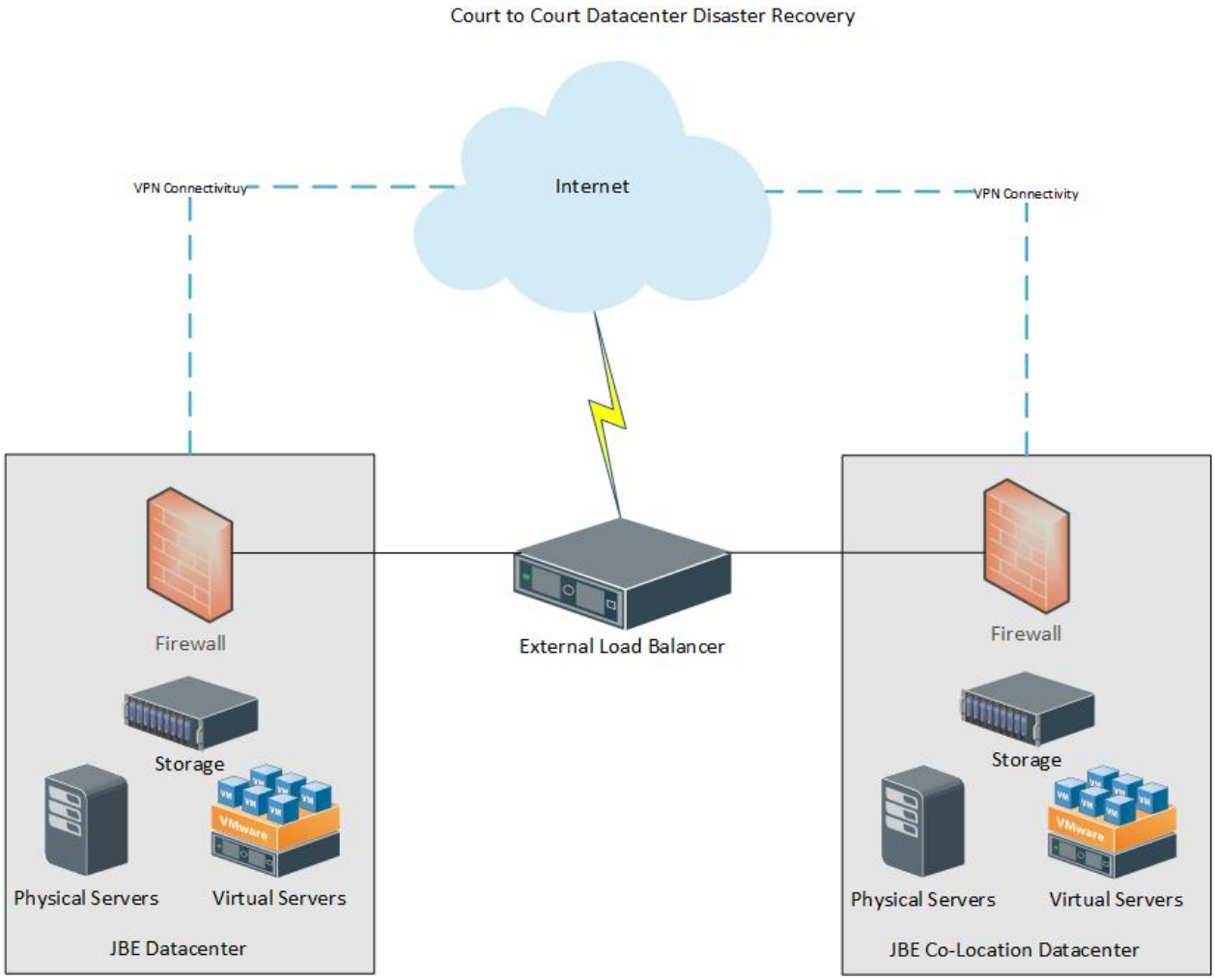


8.1.2 Scenario 2: Court-to-court colocation

Court-to-court colocation involves two similar courts in geographically diverse locations. A memorandum of understanding needs to be put into place to accommodate the complexities of this option. Implementation of this type of agreement requires a JBE to lend or borrow space in a JBE data center for racks of equipment. The JBE has to put a dedicated data circuit in the borrowed data center of an appropriate size based on requirements. In this scenario, each critical server or appliance requires a similar hardware setup, whether physical or virtual. In addition, replication has to be implemented and managed for SQL, data, and other servers. Network components also need to be in place to allow the JBE to route to the **warm or hot** redundant **sites**. Several appliances and tools can assist with running a **warm or hot site**. **Load balancers** are crucial for routing to allow the JBE to point its

server addresses to different IPs. These appliances can be set up so that if one of them is down, the external IP addresses can route to the standby **load balancer**. Other options such as hosted websites and tools that may be unavailable in the event of a disaster or outage can help in moving production.

Figure 3. Court-to-Court Colocation Diagram



8.2 Medium or Large JBE With Two or More Sites in Close Proximity

8.2.1 Scenario 1: Cloud-based DR

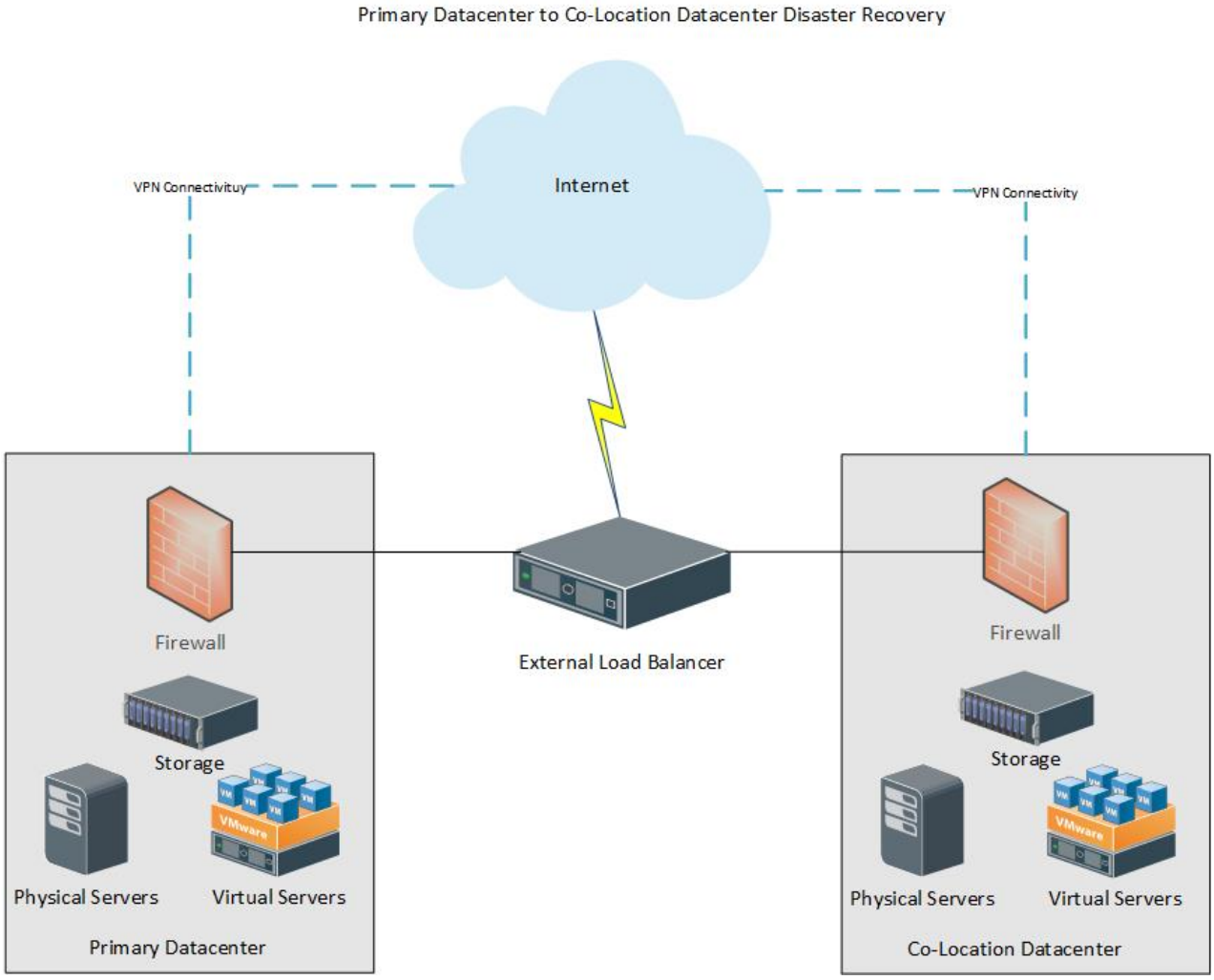
As stated in section 8.1.1, cloud-based **DR** (see figure 2, above) is the preferred **DR/BC** scenario. Depending on business need, the cloud can be used as offsite storage to replace tape backups; as a **public cloud** or **private cloud** for storage, replacing or supplementing the local SAN; or for **business continuity**, encompassing the **public cloud** and **private cloud** and introducing aspects of the **hybrid cloud** to

allow virtual servers to be synchronized on the cloud and turned up as needed during outages or disasters. **Cloud service providers** allow JBEs to replace tape backups, store tapes offsite, and virtualize data stores and critical servers and put them up on the cloud for a monthly fee plus **data ingress and egress**. The data are accessible for daily use, for recovery, or during outages and disasters. Additionally, servers can be switched from standby to active in minutes and reached as long as the Internet is accessible, functioning in the same manner as physical or virtual servers onsite. A dedicated Internet circuit (sized based on data requirements) is required to ensure that data and servers are replicated to cloud services regularly. To simplify management of data on the cloud and facilitate replication and synchronization, several types of **tapeless backup appliances** can be implemented to ensure data integrity in the cloud. And with top-tier **cloud service providers**, the JBE can often extend the internal network to the cloud, in concert with a **load balancer**, which can make failover significantly less painful.

8.2.2 Scenario 2: Colocation data center

In this scenario, a JBE uses a third-party data center to host the physical and virtual servers and appliances. Using a **colocation data center** to host data requires the JBE to install a dedicated circuit (sized appropriately per requirements) at both locations to ensure full data replication and synchronization. Each critical server requires a similar hardware setup, either physical or virtual. In addition, replication and synchronization has to be implemented and managed for SQL, data, and other services. Network components also need to be in place to allow the JBE to route to the **warm or hot sites**. **Load balancers** are crucial for routing to allow the JBE to point its server addresses to different IPs. These appliances can be set up so that if one of them is down, the external IP addresses can route to a standby **load balancer** hosted at the **colocation data center**. Other considerations include hosted websites and tools that may be unavailable in the event of a disaster or outage.

Figure 4. Colocation Data Center Diagram



8.3 Medium or Large JBE with Two or More Sites NOT in Close Proximity

8.3.1 Scenario 1: Cloud-based DR

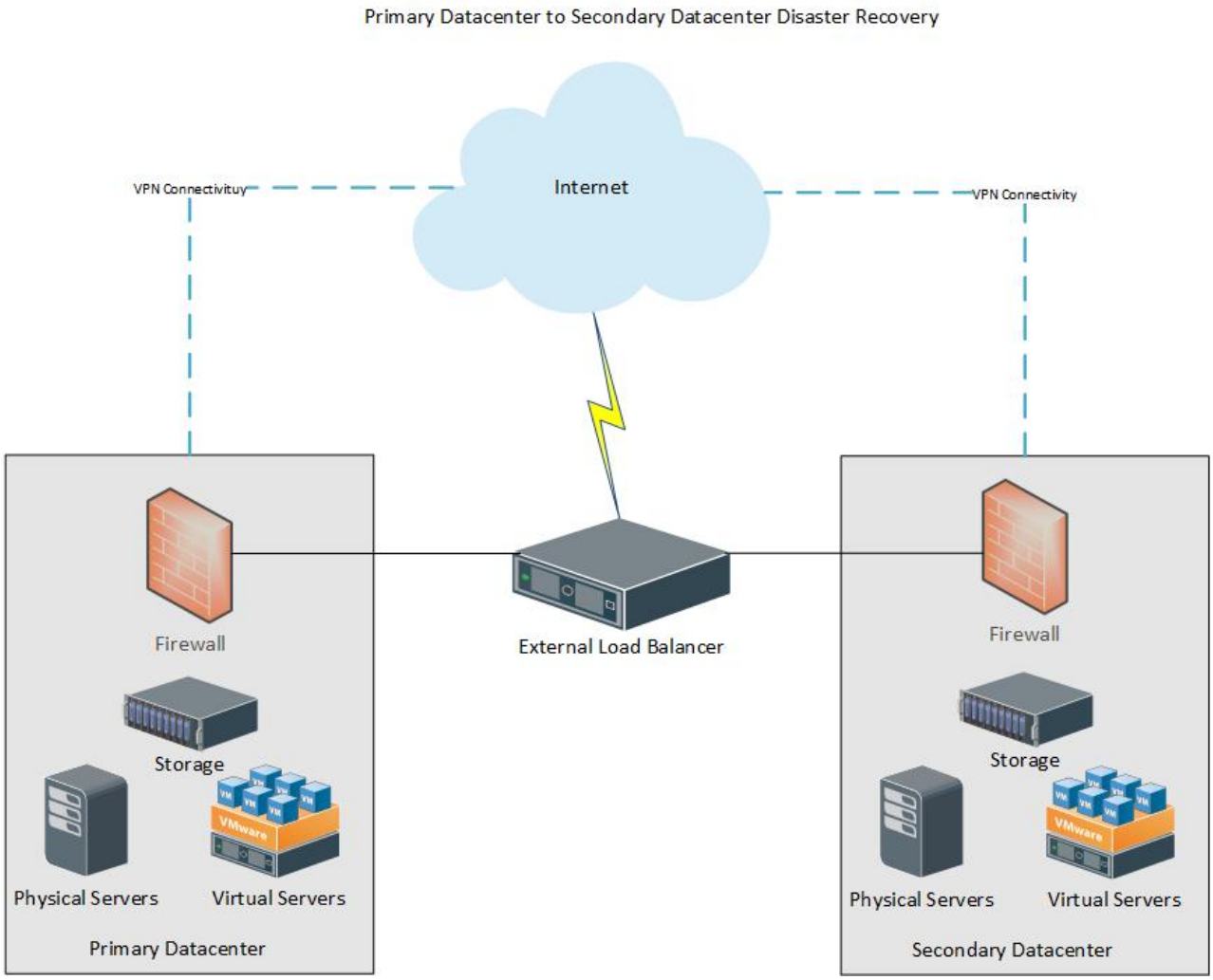
As with single-site JBEs and those with two or more sites in close proximity, cloud-based **DR** (see figure 2, above) is the preferred **DR/BC** scenario for JBEs with two or more sites *not* in close proximity. Depending on business need, the cloud can be used as offsite storage to replace tape backups; as a **public cloud** or **private cloud** for storage, replacing or supplementing the local SAN; or for **business continuity**, encompassing the **public cloud** and **private cloud** and introducing aspects of the **hybrid cloud** to allow virtual servers to be synchronized on the cloud and turned up as needed during outages or disasters. **Cloud service providers** allow JBEs to replace tape backups, store tapes offsite, and virtualize data stores and critical servers and put them up on the cloud for a monthly fee plus **data ingress and egress**. The data are accessible for daily use, for recovery, or during outages and disasters.

Additionally, servers can be switched from standby to active in minutes and reached as long as the Internet is accessible, functioning in the same manner as physical or virtual servers onsite. A dedicated Internet circuit (sized based on data requirements) is required to ensure that data and servers are replicated to cloud services regularly. To simplify management of data on the cloud and facilitate replication and synchronization, several types of **tapeless backup appliances** can be implemented to ensure data integrity in the cloud. And with top-tier **cloud service providers**, the JBE can often extend the internal network to the cloud, in concert with a **load balancer**, which can make failover significantly less painful.

8.3.1 Scenario 2: Secondary-site data center

A secondary-site data center is similar to a **colocation data center.** It uses a secondary court site as a redundant data center, which typically requires an increase in bandwidth at the secondary site as well as a dedicated data circuit (sized appropriately per requirements) between the two data centers to ensure data replication and synchronization. Each critical server requires a similar hardware setup, either physical or virtual. In addition, replication has to be implemented and managed for SQL, data, and other services. Network components also need to be in place to allow the JBE to route to the **warm or hot sites. Load balancers** are crucial in this scenario to allow the JBE to point its server addresses to different IPs. These addresses can be set up so that if one of them is down, the external IP addresses can route to the standby **load balancer** located at the secondary site as needed. Other considerations include hosted websites and tools that may be unavailable in the event of a disaster or outage.

Figure 5. Secondary-Site Data Center Diagram



9.0 PLANNING

As with any organizational undertaking, planning is an essential element in developing a solid and useful disaster recovery plan. The JBEs in California operate within a vast range of geographical, urban, and rural environments; earthquake zones and wildfire areas; and adjacencies to other JBEs. The California JBEs have varying caseloads and case types and diverse physical plants. Each possesses automation and other mission-critical support systems that differ in small or large ways from those of neighboring JBEs. For these reasons, a one-size-fits-all approach cannot work and, therefore, this document cannot specify exactly how an individual court should approach the planning effort. Each court will have its own unique set of factors to consider in developing its disaster recovery plan.

Likewise, the relative size and complexity of each court's organizational and staffing components will largely dictate the formality of the planning effort. The smallest court unit may be able to

develop a viable plan with a relatively informal and simple effort, where a large urban court may need a more elaborate and formal approach.

An important element of any DR planning effort is to first identify and thereafter coordinate as appropriate with the court's stakeholders, including internal stakeholders (judicial officers, court managers and staff, and other elements of the court family) and external stakeholders (other agencies, bar groups and law firms, vendors, and utility providers, to name a few).

In this regard, each court needs to assess the extent to which its stakeholders should be represented and involved from the outset and the level and extent of their continuing involvement throughout the planning phase. As has already been noted, what is optimal for a small rural court will likely differ significantly from what is optimal for a large urban court. Hence, stakeholder involvement should be as large and diverse as resources and practicality permit. Disaster recovery planning is most definitely an area where more stakeholder involvement is better than less.

10.0 IMPLEMENTATION

The fate of most policy and procedure manuals is to be placed on a bookshelf to gather dust. Most manuals are intended primarily for reactive reference: A discrete question comes up and a manual is pulled down from the shelf, consulted, and put back to gather more dust. Mostly, however, it stays on the shelf until a question arises.

A disaster recovery plan by its very nature, however, needs to be viewed and studied as a road map containing a cohesive set of well-thought-out procedures and steps for pre-disaster planning and preparations, continued operation during a disaster, and post-disaster response. It is intended as a tool for an organization to *prepare itself before a disaster*, as much as it is a road map for the recovery therefrom.

For this reason, it is important that the contents of the Disaster Recovery manual be widely disseminated and studied throughout the court. *All court stakeholders* who may be affected by a disaster and have a role in the recovery therefrom *should be made fully aware of the disaster recovery plan and its contents.*

As with the planning phase, described in section 9.0, the nature and extent of the dissemination and study will vary from court to court based on each court's individual environment and situation. In a small court, implementation might consist primarily of an all-hands meeting to review it and respond to questions and concerns. In the largest JBEs, such an approach is unlikely to prove practical or effective, and a more formal and involved process will be required.

11.0 KEY POINTS, CONCERNS, AND COMPLIANCE

11.1 Limited Access to & Security Controls for Backup Systems

Strict security controls and safeguards should be put into place to limit administrative access to backup systems and therefore prevent, or at a minimum – mitigate them from being compromised. Recent events, including two that have occurred in courts have further justified the importance of ensuring only one or few people (preferably executive management) maintain the master backup/recovery system(s) credentials, particularly related to access levels that allow for the backup system(s) and/or media to be wiped/deleted.

11.2 Backup of Microsoft Office 365 & Cloud Data

E-mail, hosted offsite and in Office 365, should be backed up by a trusted third-party backup service or product. Such cloud-to-cloud backups not only protect against catastrophic failure that Microsoft could experience in its data centers, but also protect the JBE against malicious or unintentional deletions of e-mail and allow for speedy recovery of e-mail. Likewise, all cloud-based OneDrive and SharePoint data including all other cloud-based critical data should be protected by a cloud-to-cloud backup solution.

11.3 Abandonment of Tapes

JBEs should be making reasonable efforts to separate from and decommission tape technologies for primary backup purposes, unless no other options are compatible with specific systems (e.g., AS/400). As budget and time permit, JBEs should also be looking to abandon tape backups *entirely*, including at secondary sites and for noncritical nonproduction data, and instead use the recommended backup media identified in this document. There are valid exceptions to this recommendation, such as if the expense and/or feasibility of increasing bandwidth to support modern backup solutions are beyond reach. JBE's can also consider cost saving approaches by repurposing production backup tape systems to be used at a secondary site or for lab/test environments. Another valid exception is to use tape as a "last resort" in case any JBE prefers to have one physical (portable) backup set on physical medium that can be securely stored.

11.4 Use of Primary SAN or Array

JBEs should never use their primary SAN and/or primary storage arrays for backup purposes. The backup environment, other than network, should be kept 100 percent separate from production storage and/or computing platforms. The only exception is for staging, test, or development systems, where a loss would not affect business operations.

11.5 Use of Virtualization Cluster

JBEs should never use their virtualization clusters, specifically a cluster served by the primary SAN or array, for backup purposes. The backup environment should be kept 100 percent separate from other resources or depend on them as little as possible.

11.6 Retention of Data (Backups)

Choosing what data to retain and how long to retain it for is a very JBE-specific decision and depends on local operating principles, local SLAs, budget for appropriate backup resources, infrastructure, and laws and rules. As with document destruction, an appropriate backup architecture should be implemented at a court that supports the JBE's retention and/or destruction requirements and aligns to the business drivers to which the JBE has committed.

IMPORTANT NOTE With recent catastrophic and visible events in industry where data hostage and data corruption situations have occurred, it is of utmost importance that JBE's completely understand the architecture and working principals of their backup and DR system(s) to mitigate any chances of corruption and/or maliciously encrypted data being the only backup copy of a JBE's data. In order to avoid such a situation (e.g. sleeper code, or maliciously encrypted data), a JBE may wish to keep full copies of backups for certain periods of time and taken at different intervals (e.g. 6 months, 12 months, etc.), and 100% isolated from the production network.

11.7 Data Classifications

This framework covers the process and methods for data classification only in part, because that focus is typically a balancing act between compliance, discovery, and protection. However, larger JBEs will find that classifying data will help reduce any consumption or utilization constraints around SANs, disks, backups, and high-availability solutions. The rules for data and compliance are very specific, and so at each JBE, intake and classification of the data from various sources, such as those that follow, are important:

- **Payment Card Industry (PCI)**. Reference PCI resources and/or your merchant account provider for relevant information.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**. Reference HIPAA resources and/or your local county for relevant information.
- **California Law Enforcement Telecommunications System (CLETS)**. Reference CLETS documents or contact your CLETS contact for relevant information.

11.8 Purpose-Built Backup Appliance vs. Backup Server

The industry allows JBEs to select any available backup solutions that meet their needs and align to the Judicial Branch *Disaster Recovery Framework*. JBEs should assess their environments to select an appropriate backup solution that presents the fewest risks and is least disruptive to ongoing management efforts. Some backup solutions are designed as purpose-built appliances (non-Microsoft) rather than traditional Microsoft Windows servers with a backup software application installed. Purpose-built appliances are recommended over traditional Microsoft Windows backup servers because they are immune to or far less affected by common-environment outages (Microsoft's Active Directory and the like) and less susceptible to malware targeted specifically for Microsoft-based servers. In a crisis, dependencies can impede recovery activities and compromise a JBE's ability to focus on restoration of data.

11.9 Cloud Service Subscriptions and Payments

Based on how the California State Controller's Office (SCO) operates, in addition to the time it takes for invoices and approvals for payment to work their way through the process, payments to contracted vendors and organizations can often be delayed. Many vendors require payment in full within 30 days of receipt of goods (Net-30), whereas the SCO pays on terms of Net-45 at best. The delay of payment can introduce complications with JBE cloud service subscriptions. When a JBE contracts with a cloud service provider, the JBE should carefully review the contract and/or agreement terms and conditions regarding what happens with a customer's data following a delayed payment. For example, when the Legislature and Governor's Office experience delays approving the California budget, delays of payments have historically resulted for many vendors. Whereas local infrastructure is a capital expenditure and is less affected by delayed payments, cloud infrastructure and services are operating expenses and rely 100 percent on timely payments.

11.10 Uncompromised Access to Credentials for Recovery Systems and Cloud Platforms

It is essential for JBEs to plan and be prepared for the worst of circumstances. JBEs should implement a credentials locker, credentials list, and so on, and store them in a documented and secured location away from and off of any IT system or facility that could be compromised and result in the activation of a JBE's recovery plan. Should a JBE's IT environment be compromised based on an IT failure, facility failure, or natural disaster, uncompromised access to credentials is mandatory to ensure that the JBE can access its backups and other DR-related systems. The JBE's credentials should be kept alongside the JBE's disaster recovery plan. JBEs should always lean on a multifaceted approach to where mission-critical documentation (e.g., credentials and DR plan) is stored and located in case

access to anything and/or everything could potentially be impeded and/or permanently inaccessible until recovery.

12.0 MONITORING, TESTING, VALIDATION, AND REVIEW

A JBE's backup strategy and DR strategy (if applicable) should be comprehensively tested *at least* once per calendar year. The sophistication or simplicity of the DR solutions in place at each JBE is irrelevant to this recommendation. Of course, a JBE may choose to test more frequently if desired, and should implement a more frequent testing exercise if any uncertainty or lack of integrity exists with the backup and/or DR solutions in place.

12.1 Regular Review of Backup and Disaster Recovery Systems

12.1.1 E-mail notifications

E-mail notifications for alerts and other information should be set up in each system that makes up a JBE's DR solution. These e-mails should be reviewed regularly (e.g., daily) and checked for errors and completeness.

12.1.2 Backup job monitoring and auditing

A responsible person, persons, or team should be assigned the task of auditing all backup jobs on a JBE's backup system on a regular interval. Doing so will ensure that any new systems brought into the environment have a second and certain chance of being captured within the backup and DR plan.

12.1.3 Site recovery/cutover systems monitoring and auditing

A response person, persons, or team should be assigned the task of auditing all site recovery systems on a regular/repeat interval. Doing so will ensure that any new systems brought into the environment have a second and certain chance of being captured within the site recovery and DR plan.

12.1.4 Gap Analysis

A gap analysis should be performed regularly (e.g. quarterly or within reason) to serve as a "catch-all" mechanism in addition to the above routine checkpoints. The gap analysis will also lend to ongoing refining of a JBE's backup and DR strategy and allow for continual planning, budgeting and changing.

12.2 Routine Testing Exercises

JBEs should establish a testing plan or testing effort and execute a routine testing exercise on a regular interval, but no less frequent than once per calendar year. Testing exercises help

provide peace of mind, but more important, they prove that backup and site recovery systems are working as designed and will work should they be needed in a real scenario. Although most systems allow for out-of-band testing and data-redirect without affecting production performance or data, outages may be required for testing and should therefore be included in the test plan.

12.3 Testing Simulations

12.3.1 Loss of building access

In addition to routine and general types of testing, JBEs should run simulations that reflect real-life possibilities. One simulation is to react to a full loss of building access—specifically, the building that houses the JBE's data center. In this test, ideally, an IT team would consider working offsite or from another building.

12.3.2 Loss of access to all systems (onsite or offsite) based on catastrophic outage or disaster

In addition to routine and general types of testing, JBEs should run simulations that reflect real-life possibilities. One simulation is to react to a full loss of all systems either at the JBE's primary data center, the cloud, or both. In this test, ideally, an IT team would consider working offsite or from another building.

12.3.3 Backup system failure

In addition to routine and general types of testing, JBEs should run simulations on recovering data when their primary backup appliances or systems have failed but all other production systems, including secondary replicas of backups, are operational.

12.3.4 High-availability (site recovery) system failure

In addition to routing and general types of testing, JBEs should run simulations on remediating systems in the event that their primary site recovery systems have failed and cannot function as designed.

APPENDIX A

LIST OF HIGH-LEVEL TECHNICAL REQUIREMENTS AND SYSTEMS/DATA CATEGORIZED BY RECOVERY TIME

RECOVERY-TIME DISCLAIMERS

- Recovery time depends on the following:
  - The actual disaster (severity)
  - Whether the facility or physical access is affected, including safety situations (e.g., hazmat, fire, smoke)
  - Staff capacity and availability
  - Replacement equipment (if applicable)
  - Conflicting DR recovery commitments or plans (e.g., CCTC or other data centers/cloud)
  - Recovery actions, such as abrupt responses that could lead to some or significant permanent data loss based on available backups, the approach taken for data restoration, and/or disaster recovery site cutovers
- Fault tolerance is typically costly and requires additional hardware and software.
- Some functionality or components are built into other component systems (overlap of functionality).
- Time to recover (TTR) is the maximum recommended/defined outage time for purposes of implementing priorities for data recovery and outage mitigation.
- Hardware items on the end-user side of IT (e.g., printers, desktops, scanners, barcode readers, etc.) have not been included because they are considered end-user equipment and are outside the scope of the disaster recovery framework.

HIGH-LEVEL TECHNICAL REQUIREMENTS

- TTR of 12 hours maximum
- Infrastructure (network, Active Directory (AD), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP))
- Shared/combined storage (SAN, etc.)
- Virtual hypervisor/platform
- Backup solution/platform
- Wi-Fi

- Load balancers
- Reverse proxy

BUSINESS RECOVERY REQUIREMENTS (EXAMPLES OF SYSTEMS AND SERVICES)

The tiers below align with the judicial branch Next Generation Hosting Strategy Workstream's output, except in ways that clearly delineate how approaches to disaster recovery differ from hosting and uptime, given that all are interrelated and depend on one another for the reliability and protection of data.

- **TIER 1**—HIGH priority; TTR (not considering disclaimers) of 12 to 48 hours maximum; and systems and services as follows:
  - VoIP
  - Case Management Systems (CMS)
  - Document Management Systems (DMS)
  - File servers (holding judicial, executive, human resources, finance, and IT data and documentation)
  - E-mail (systems dependent on e-mail, such as alert and public communication systems), Microsoft Office 365, and others
  - Public website (hosted on-premises or offsite); important for a mechanism to broadcast information to the public and for the public to send or input data to the court; the portal at each court
  - Electronic reporting, docket, and minutes
  - Jury management system (JMS)
  - Virtual private network (VPN)
  - Electronic Probable Cause Declaration (ePCD)
  - Electronic Search Warrants (eWarrant)
  - Interfaces (interagency; some e-filing)
  - Building access control (e.g., Identiv, Schneider Electric)
  - Finance systems on-premises
  - Human resources systems on-premises, time card systems, Phoenix/SAP
  - Jury instructions
- **TIER 2—**MODERATE priority; TTR (not considering disclaimers) of 48 to 72 hours maximum; and systems and services as follows:
  - Intranets
  - File servers (holding less- or moderately important data)
  - Print servers
  - Building automation system
  - California Courts Protective Order Registry
  - CLETS
  - Department of Motor Vehicles access, controls or interface

  - Other interfaces: various justice partners (e.g., Franchise Tax Board, Department of Justice, district attorney, police department, California Highway Patrol, sheriff, etc.)
  - Site control (elevator controls, door controls, etc.)
  - Electronic transcript assembly tools/software
  - Interactive voice response (traffic, jury, etc.)
  - Electronic signing product/solution
  - Middleware
  - Reporting systems (not built into CMS, but standalone)

- **TIER 3**—LOW priority; TTR (not considering disclaimers) of 168 hours maximum; and systems and services as follows:
  - IT tools and unique IT management systems (e.g., help desk, logging, controls, and network/system/application monitoring)
  - Video surveillance
  - Meeting systems (WebEx, Skype, etc.)
  - Digital signage
  - Queuing systems
  - Mobile device management

APPENDIX B

RECOMMENDED MINIMUM REQUIREMENTS FOR A BACKUP SOLUTION

Note: Tape should never be used as the primary backup medium.

- Disk-based
- Cloud-based
- Cloud-to-cloud backup capabilities for Microsoft Office 365 (e.g., OneDrive, SharePoint, Exchange Online) backups
- Sufficient Internet bandwidth for cloud and/or remote backups
- Scalable (can grow as court grows without large, repeated capital expenditures)
- Granular backup and restoration (e.g., exchange items in mailboxes, SQL objects, individual files)
- Ability to create multiple schedules
- Ability to notify or alert IT staff of problems
- Ability to verify backups
- Ability to restore to a different backup target
- Ability to encrypt sensitive or classified data or information
- Ability to audit all changes made to the backup system, backup jobs, schedules, etc.
- Ability to create multiple backup jobs
- Ability to create backup schedules with multiple backup targets
- Ability to replicate *offsite:*
  - To the cloud
  - To a secondary backup system
  - To a removable or portable disk
  - To tape (*as last resort*)
- Ability to initialize or mount a backed-up virtual machine in the cloud (specific for cloud backup solutions)