TERMINAL LABS

Executive Summary

ERP Disaster Recovery Evaluation

Report for:

Sample Inc.

Kalamazoo Site

Site: Kalamazoo

The following is an overview of the Disaster Recovery Plan (DRP) analysis for the Kalamazoo site. This site employs IQMS for Enterprise Resource Planning (ERP).

Methodology

Sites have been scored across eleven disaster scenarios. Each scenario has been rated on the efficacy of the DRP if carried out successfully. Scoring examines **Data Preservation**, and **Service Restoration** plans, and the **Documentation,** and **DRP Testing** in place supporting these plans. These ratings range from A to F, with A being an ideal recovery, and B and C being fair, but with clear room for improvement. Finally, D and F note marked concerns.

Evaluation Overview

Kalamazoo site has robust onsite backups, but lacking documentation for restoring from those backups. Restoration is dependent on staff that may not always be accessible. Adequate documentation should exist for trained operators to be able to restore from backups even when key personnel with some tribal knowledge may not be available.

There are **no offsite backups** for this site. While onsite backups will protect against many incidents, offsite, air gapped backups are required to mitigate against: catastrophic hardware failures, ransomware attacks, site damage, and onsite malicious actors. A process for offsite backups and restoration from these backups must be put in place, documented, and regularly tested.

Onsite backup power generation is available, but no provision has been made for a WAN backup in the event of external internet outage. The ERP system currently has no documented need for WAN access, but this will at minimum become a requirement when an offset backup process is put in place.

The site has **no backup server hardware** on site. Failover hot swappable hard drives are available, but there are no backup servers available to be spun up in the event of a hardware failure. There is a vendor in place to provide server maintenance, but their service contract does not guarantee uptime without the provided RTO. New contracts should be negotiated with vendor RTO or provision should be made for the onsite team to handle server hardware failures.

Kalamazoo Ratings

Disaster Scenarios		Data Preservation	Service Restoration	Documentation	DRP Testing
Human Disasters	Misconfiguration	C	C	C	D
	Missing Operator	N/A	D	B	F
Technical	Network Outage	C	C	D	F
	Server Failure	C	C	A	F
	Application Failure	B	B	A	C
	Data Corruption	D	D	B	C
Natural	Electricity Outage	A	A	A	A
	Internet Outage	B	B	F	F
	Site Damage	C	C	A	A
Hostile Actors	Ransomware and Hacking	D	D	C	F
	Malicious Destruction	D	D	B	D

Next Step Recommendations

Paragraph Summary of recommendations based on the evaluation

Add offsite backup

Better documentation and training so that more staff can achieve backup restores

Regular testing of all elements of DR plans

Proper configuration of onsite and offsite backups to make them more resilient to ransomware type attacks

Hardware on hand for quick server replacement and documentation for the process

Configure ERP database for transaction logging.

Configure backups to be immutable and air gapped

Priority and Time ratings

These ratings are **global** even though the to-do list is grouped for the taskings logical relationship to one another.

Priority

[high] High ratings are either because of low time commit for good pay off, or longer term project that shores up weaknesses in the DRP

[med] These objectives ensure the house is in order for the DRP with training and instructions, or improved digital architecture.

[low] These tasks should not get in the way of operations and be considered tasking for downtime periods.

Time

[quick] A couple meetings and discussions to confirm consensus

[short] Less than a month

[mid] Less than 6 months

[long] Greater than 6 months

Site Recommendations:

A.	Human Disasters			
	1.	[high]	[mid]	Set up, and properly configure offsite, air gapped backups.
	2.	[med]	[short]	Create robust documentation for existing onsite backup restoration.
	3.	[med]	[mid]	Train staff on new onsite backup documentation to reduce bus factor.
	4.	[med]	[mid]	Regularly test the backup restoration process.

B.	Technical			
	1.	[high]	[short]	Establish, document and test onsite options for server restoration.
	2.	[high]	[short]	Work with hardware vendors to ensure the service is provided will enable established RTO.
	3.	[med]	[short]	Establish, document, and test process for setting up backup WAN access in event of external internet outage.
	4.	[high]	[mid]	Set up, and properly configure offsite, air gapped backups.
	5.	[high]	[short]	Configure ERP database to use transaction logs.
	6.	[high]	[short]	Create documentation for and establish regular testing for restoration from onsite backups.
	7.	[high]	[short]	Create documentation for and establish regular testing of restoration after application level failure.

C.	Natural Disasters			
	1.	[high]	[short]	Establish, document and test onsite options for server restoration.
	2.	[high]	[short]	Work with hardware vendors to ensure the service is provided will enable established RTO.
	3.	[med]	[short]	Establish, document, and test process for setting up backup WAN access in event of external internet outage.
	4.	[high]	[mid]	Set up, and properly configure offsite, air gapped backups.

B.	Hostile Actors			
	1.	[high]	[mid]	Set up, and properly configure offsite, air gapped backups.
	2.	[med]	[short]	Establish, document, and test process for setting up backup WAN access in event of external internet outage.
	3.	[high]	[short]	Configure ERP database to use transaction logs.
	4.	[high]	[short]	Configure off site backups to be immutable.
	5.	[high]	[mid]	Create documentation for and regularly test / practice restoration from air gapped backups to simulate recovery from ransomware attack.