



Disaster Recovery Self-Audit

WHITE PAPER

Disaster Recovery Audit

There are 3 steps to this process:

1. Identify all data and IT-related functions (like credit card processing, documents on your file server, member web portal, a CRM system, critical applications, etc.) you have in place.
2. Classify the **importance** of the data and functions you've identified.
3. Apply an appropriate backup and disaster recovery plan to match the value and importance of each asset.

Use the following rating system on the impact to your business if you suffered a significant outage or complete loss of the data and processes you've identified:

0% = Zero Impact

20% = Annoying but Recoverable

40% = Minor Damage with Loss

60% = Disaster with Considerable Loss

80% = Major Disaster with Significant Loss

100% = Total Loss

When assessing costs, be sure to factor in loss of tangible sales, client goodwill, costs for re-keying (typing) the data (or any other recovery costs) as well as legal costs associated with failure to deliver on contractual obligations, potential lawsuits, etc.

| Data Or Business Function | If you lost access to this data/functionality for a week or more, what impact would it have on your business? | If you lost this data/functionality permanently, what impact would it have on your business? | Estimated Cost (Include cost of recreating data, entering it, loss of business, etc.) |
|----------------------------------|--|---|---|
| Accounting Information | | | |
| Client Data (CRM) | | | |
| E-mail | | | |



SAALEX INFORMATION TECHNOLOGY, LLC.

THE IT EXPERTS—WHY TRUST ANYONE ELSE?

| | | | |
|--------------------------------------|--|--|--|
| Contracts And Legal Documents | | | |
| Custom Software and Code | | | |
| Web sites and content | | | |
| Video and Audio recordings | | | |
| Total Costs: | | | |



Determine Your Risk Score

| | | | | | |
|---|-------|--|--|-------|--|
| How often do you perform a full back up? | | | How often are your backups tested and validated? | | |
| Every hour | - 200 | | Every day | - 100 | |
| Every day | - 100 | | Weekly | + 50 | |
| Weekly | + 100 | | Monthly | + 100 | |
| Monthly | + 200 | | Never | + 200 | |
| Do you keep paper records (or scans) you could reference as a source for re-entering lost data? | | | Is your data centralized onto on server or location or scattered across multiple devices and locations? | | |
| Yes | - 100 | | Consolidated | - 100 | |
| No | + 100 | | Scattered | + 100 | |
| Who has access to your computer network? (Check all that apply) | | | How are your backups done? | | |
| Trusted, computer-savvy employees | - 100 | | Automatically, offsite | - 100 | |
| Trusted IT support company | - 50 | | Manually by a skilled IT person | + 50 | |
| Unskilled workers/transitional staff | + 100 | | Manually by an admin | + 100 | |
| Cleaning crew, maintenance | + 200 | | Not sure | + 200 | |
| Where is your data stored? | | | How long do you keep a copy of your data? | | |
| Don't know | - 200 | | Forever | - 100 | |
| On tape drives, USB devices | - 100 | | One year | - 50 | |
| Onsite hard drive | - 50 | | Under a year | + 50 | |
| Offsite in the cloud | + 100 | | We use the same tape/device daily | + 100 | |
| Do you live in an area or office building that has experienced any of these disasters OR that has a high potential for one of these disasters to occur? (Check all that apply) | | | Do you or any of your employees have the ability to do the following? (Check all that apply) | | |
| Tornado, hurricane or severe storm | + 100 | | Download files from the Internet | + 100 | |
| Earthquake | + 100 | | Install non-company approved software | + 100 | |
| Terrorist attack | + 100 | | Delete files from the server | + 100 | |
| Fire/problem with another tenant | + 100 | | Access your server remotely | + 100 | |
| Flood | + 100 | | Create/change their own password | + 100 | |



SAALEX INFORMATION TECHNOLOGY, LLC.

THE IT EXPERTS—WHY TRUST ANYONE ELSE?

| | | | | |
|--|-------|---|-------|--|
| Do you store sensitive data that must be protected by law? (Medical records, credit cards, social security numbers, financial data, etc.) | | Do you have a trusted, professional IT person or firm monitoring your network DAILY for security threats and failed backups? | | |
| No | - 100 | No | + 200 | |
| Yes | + 200 | Yes | - 200 | |
| Do you routinely download and backup all data stored on 3rd party cloud applications (web site files for example)? | | Do you have a “break the glass” document for what should happen if a senior executive dies or is disabled? | | |
| Yes | - 200 | No | + 200 | |
| No | + 200 | Yes | - 200 | |
| How old is your server and/or other workstations that contain <u>critical</u> data? | | Do you have the following in place (check all that apply): | | |
| Under a year old | - 100 | Signed, acceptable use policy & training | + 50 | |
| 1-3 years old | + 50 | Monitoring software for the network | + 100 | |
| 3-4 years old | + 200 | Mobile device policy and monitoring | + 100 | |
| Over 4 years old | + 300 | Up-to-date anti-virus & threat monitoring | + 100 | |
| | | A firewall that is monitored & updated | + 100 | |
| Regarding disaster recovery and business continuity, check all that apply: | | | | |
| You DO have a written disaster recovery plan | - 200 | You DON'T have a disaster recovery plan | + 200 | |
| You review & update your plan regularly | - 100 | You DON'T update your plan | + 100 | |
| You conduct periodic tests of your plan | - 100 | You DON'T test your plan ever | + 100 | |
| You DO have an inventory of assets for insurance | - 100 | You DON'T have an inventory of assets | + 100 | |



Scoring:

0 Or Less: Low To No Risk

You either don't have very much critical data on your computer or your backup plan is well designed. If this exercise revealed one or two areas you are NOT securing well, you now have the opportunity to resolve those areas immediately.

0-200: Medium Risk

Depending on what data is compromised, you will most likely be able to recover it without major catastrophic costs or consequences. HOWEVER, there are certain areas that are more important than others. For example, if you had sensitive data lost or stolen, the consequences from that could be extensive in the form of legal fees, lost customers, lost market share, a harmed reputation and possibly even a lawsuit.

200 Or More: High Risk

Your business is extremely vulnerable to various data-erasing disasters, and there is a high chance that you would NOT be able to recover it at all. It is imperative that you strengthen your current backup, security and disaster recovery plan immediately.

"93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately."

(Source: National Archives and Records Administration in Washington)

