Managing Service Provider Risk Worksheet

enchant

Instructions

This worksheet will help you manage risks associated with service providers that your company depends on.

Step 1: Identify the service providers

Think about all the ways money flows in and out of the company. Those flows of money are typically going to or through service providers that your company depends on.

Some examples of service providers:

- The payment processor that vaults and charges customer credits cards
- The web hosting provider that hosts your website
- The shipping provider that delivers your products
- The email provider that you use to deliver transactional emails
- The content distribution network you use to speed up your website

Step 2: Prepare a risk profile for each service provider

Disruptions caused by a service provider can result in significant and unexpected harm to your company.

To identify and quantify these risks, print out and fill out the Service Provider Risk Profile form (later in this document), once for every service provider. A sample filled out risk profile form is also included in this document.

Explanation of the fields:

- **Value Provided:** What does this service provider do for your company?
- **Type of Risk:** What could happen with this service provider (intentionally or unintentionally) that would cause harm to your company?
- **Risk Level:** How much harm would your company feel if this type of risk were to occur? Low, Medium or High
- **Lock In:** Is there some reason why you're stuck with this service provider? How have they locked you in?
- **Alternatives:** What reasonably similar alternatives exist to this service provider?
- **Replacement Effort:** How much effort would it take to stop using this service?
- **Exit Strategy:** If you needed to stop using this service provider, what's the plan?

Step 3: Analysis and Actions

A set of service provider risk profiles gives you a starting point for broader conversations at your company:

- What amount of risk is acceptable to your company and customers?
- How can you mitigate risks that you've deemed unacceptable?
- What measures can you put in place to prevent your company from taking on unacceptable risks in the future?
- ...and so on

Step 4: Update the risk profiles yearly

Creating risk profiles isn't a one time thing. We've found the need to update our risk profiles yearly. How often you need to do so depends on the rate at which your company evolves.

We've had to update our risk profiles when:

- previously identified risk levels could be lowered because of effort put into mitigating the specific risks. For example, adding extra backups to mitigate against data loss
- previously identified risk levels needed to be increased due changing business conditions (eg: taking on larger customers with higher expectations)
- new risks are identified as our business usage and requirements change

Service Provider Risk Profile

Service Provider:	Date Completed:
Value Provided:	

Identified Risks

#	Type of Risk	Risk Level	Notes
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			

Lock In
Alternatives
Replacement Effort
Exit Strategy

Service Provider Risk Profile
(Additional Risks)

Service Provider:	Date Completed:

Identified Risks

#	Type of Risk	Risk Level	Notes

Service Provider Risk Profile
(SAMPLE)

Service Provider: *AWS S3*	**Date Completed:** *Feb 25, YYYY*
Value Provided: *block storage for raw incoming emails*	

Identified Risks

#	Type of Risk	Risk Level	Notes
1	*System outage for 3 hours*	*Medium*	*Partial disruption*
2	*System outage for 24 hours*	*High*	
3	*Partial loss of data*	*Medium*	*Mitigated*
4	*Full loss of data*	*High*	*Long time to restore*
5	*Data disclosure due to security breach*	*High*	*GDPR*
6	*Degraded system performance for 3 hours*	*Low*	*Partial disruption*
7	*Degraded system performance for 24 hours*	*Medium*	*Partial disruption*
8	*Suddenly ceased to operate*	*High*	*Unlikely*
9	*Failure to abide by privacy laws*	*High*	*GDPR*
10			
11			
12			
13			
14			
15			
16			
17			
18			

Lock In

S3 has little lock in, other cloud providers offer equivalent services. However, we want to keep our primary compute instances near our block storage.

Alternatives

Google Cloud Storage, Microsoft Azure Storage.

Replacement Effort

Integration effort is low for new data. However, it would take some time to restore existing data into an alternative.

Exit Strategy

Migrate to an alternate provider.

Better customer conversations start with Enchant

Go to Enchant.com