# Risk Mitigation Strategies

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Mitigation</td>
<td>2</td>
</tr>
<tr>
<td>Service Level Agreements (SLA)</td>
<td>3</td>
</tr>
<tr>
<td>Service Level Agreement Considerations (For Operational Risks)</td>
<td>4</td>
</tr>
<tr>
<td>Service Level Agreement Considerations (For Technical Risks) - 1</td>
<td>6</td>
</tr>
<tr>
<td>Service Level Agreement Considerations (For Technical Risks) - 2</td>
<td>8</td>
</tr>
<tr>
<td>Local Risk Mitigation Strategies</td>
<td>9</td>
</tr>
<tr>
<td>Notices</td>
<td>11</td>
</tr>
</tbody>
</table>
So risk mitigation, we'll talk about service level agreements, and certain considerations.
Service Level Agreements (SLA)

Service Level Agreements (SLA)

The most important tool to ensure that your needs are met.

If it isn’t specified in the SLA, there is no guarantee that it will happen.

Make sure that any concerns or special needs are addressed.

**030 We saw this a bunch. I’m not going to beat this slide to death too much. But the bottom line here is, if you have certain requirements for your organization, for your data, you need to ensure that any service agreement, or service provider adheres to those same sorts of requirements, whether it’s cloud computing or any other type of service. So what can we do from an operational standpoint?**
Service Level Agreement Considerations (For Operational Risks)

Service Level Agreement Considerations (For Operational Risks)

The cloud provider should

- Provide financial insurance for lost data, lost sales, or even potentially a negative impact to the customer’s reputation due to outages or breaches
- Allow transparency into the overall information security and management practices
- Establish a documented security breach notification processes with the customer
- Allow service level agreements for patching and vulnerability remediation
- Provide the customer with documented regulatory compliance assessment results
- Provide customers with the ability to specify where and what jurisdictions their data is allowed to be stored in

**031 We want to ensure there's transparency. We want to be able to see the environment. Can I view the environment, can I-- do I know what you say is taking place, in terms of backups and physical controls? Are those actually being adhered to? Do I know all those policies? Do I know your backup policies? The one thing, the exact location, like, Amazon, I pick on them a lot, because they're leading in the cloud computing space. You know, the exact location of each data center, and what information is available, the controls in that data center, it isn't as transparent as maybe you would want it to be. They say, yeah, we do it according-- were SaaS-70 audited or we're compliant in this regard, but what are the exact controls, how are they implemented, you may not have access to all that information.**
What are the notification procedures if there's a breach? You know, if somebody else within my organization, or within my service provider is compromised, is there risk that I would also be compromised, and do I need to be notified of that? You know, if somebody is going to try to access my data in law enforcement, what are the procedures for me being notified of them accessing my data? Those are things that you want to be aware of.

Patching is another one. That's a big deal. If you're this probably goes more toward the platform as a service piece, because if you're using the infrastructure as a service piece, you're still responsible for your own patching in most cases, unless you're paying extra for a service that manages your box for you, your virtual box. But when is that patching actually taking place, and am I getting notified? Is there a change in management that is associated with that? Is it logged? What happens if something breaks, what's the backup procedure, restore procedures. Certainly you want to be cognizant of those sorts of things.

Yeah, the last bullet there is interesting. Do I have the ability to move my instances around? It depends. I gave you a couple of examples of that already.

The insurance is a big one. You know, you should have, as a company, as-- government is kind of a little bit different, but as an independent company, what sort of insurance do I have if something happens to that data, or my resources aren't available, and you know, I start to lose business, or revenue. Am I-- you
know, does that service provider also have insurance to provide some sort of compensation if that actually occurs.

Again, it falls in line with whatever things that I have to regulate me, or support me or my organization, we need to push some of those off on the service provider to make sure that they adhere to those things again.

**Service Level Agreement Considerations (For Technical Risks) -1**

Service Level Agreement Considerations (For Technical Risks) -1

The cloud provider should

- Wipe persistent media before it is released into the pool at the request of the customer
- Provide the customer with documented backup and retention strategies, as well as, records of tests to restore the backups
- Allow the customer to encrypt sensitive data using keys that the cloud provider does not have access to
- If possible, dynamically reallocate resources to increase support for defensive measures when an attack is taking place
- Divert resources to filtering, traffic shaping, and analysis during a suspected DDoS attack

**032 Technical controls are things that need to be in place. Wiping persistent media. What are their policies for doing it? When I shut down an instance, or I have-- you know, kill a database that I no longer need, what are their policies for wiping that data off of there? Do I have to notify you, or does it happen automatically? Are things encrypted during storage or just in transport? There are some providers, there’s Zetta, Z-E-T-T-A Enterprise Cloud**
Computing. They actually have-- their policy is that they actually have FIPS compliant encryption on the disk by default. Other places you have to actually implement, maybe, Windows EFS, or some other-- or TrueCrypt, or some other encryption to actually encrypt your data at rest. What are the policies for that? How does that work? Is it done automatically, or is it something that I need to do. Those are important things to understand.

Yeah, what are the opportunities, or administrative capabilities that I have to rapidly provision elsewhere? If something happens to my instance, how quickly can I recover? Are there little-- I'm saying, do I have the ability to, you know, pick a point in time, and restore from that point in time, which you can do pretty easily in a virtual environment, say, hey, I think the compromise happened yesterday, let me roll back to the day before yesterday, and restore from there. How easily can I do those sorts of things, are important things to consider in a cloud environment.

The firewall thing is an interesting concept for me as well, just in an old school collocation environment, or where you're managing the firewall, part of your best practices are to see where you're getting attacks from or you're getting scans or denial of service attacks, and regularly going through and maybe blacklisting some of those addresses at the router, or whatever the case may be.

What sort of things do you have to support those requirements in a cloud computing environment? Do you have access to those firewall controls to do some blacklisting, to do some additional
monitoring? Those are things that you certainly want to consider.

**Service Level Agreement Considerations (For Technical Risks)**

The cloud provider should

- Log and audit customer access to cloud resources
- Provide a method for the customer to perform forensic analysis on resources if necessary
- Allow the customer to conduct vulnerability scanning and configuration audits if required for regulatory compliance

**033 I mentioned logging, and in the Amazon perspective for, you know, the responsibilities of the customer, it is important for you to understand that, just because you're going to a service provider, doesn't necessarily mean you're outsourcing that security as well. You may, they may have a service that does that for you, but in general, you need to understand that there's things that need to happen, file integrity monitoring needs to take place in your environment, depending on your requirements, of course, but you know, host based firewalls, you still want to make sure host based firewalls are implemented and that they're configured appropriately, you still want to do patch management, you still need antivirus, you still need host
intrusion prevention, you still need an application firewall, perhaps, right? You still need to have some sorts of log management, log collection, right? And you need to be able to monitor that for any kind of anomalies or alerts. I mean, those are still things that need to be done, and you can implement those in the same cloud computing environment, and the same security group, or you can implement some of those things externally, depending on what some of your configuration options are.

Local Risk Mitigation Strategies

Data

- Consider the value of the data prior to determining if it needs to be in the cloud or should be stored locally.
- Consider backing up critical data locally in the event that the cloud provider permanently loses the data.

Employees

- Provide training, policies, and procedures to employees accessing the data to mitigate accidents.
- Restrict access to only what an employee needs to do their job.

Connections

- Ensure a secure and reliable connection to the cloud provider.
- Consider configuring traffic between the organization and provider to be a priority.

**034 So local risk mitigation strategies, local, meaning things that you can do on your end. A lot of it comes back to understanding your data. What sort of information do I process, what are the controls that need to be placed upon my data regardless of where it is, and ensure that the service provider does those
same sorts of things for me. Employees need to understand what the difference is of where that data resides, where the application resides, and generally safe processing habits, whether it’s accessing, like I said, Google Docs, or something like that, over https, or whether it’s making sure that, as I transfer that information, it’s going over that secure connection, or that those-- the information is encrypted, that I’m not pulling it down to a different box, and leaving it on my host. There’s different types of things, depending on the computing environment and the data, that your employees need to be aware of.

And again, making sure that you have good bandwidth, right? As soon as you-- and it depends, again, on what you’re outsourcing, or you’re putting out in the cloud, you may need to have additional bandwidth assigned or set up within your infrastructure to maintain that connection to your development environment, or your production environment to support it.
Notices

© 2016 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government’s rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.