

Your Name: Nathan Rickett
Risk Identification Exercise
Project: The data center I am working at is in the process of migrating systems from on-premises to AWS.

Rank	Risk Name	Description	Triggers	Potential Responses	Prob. of Being Triggered (%)	Impact if Triggered	Chosen Response
1	Network interruption	Migrating systems to cloud will result in relying on internet connection due to AWS being reachable via an internet service provider. A stable connection will be crucial when migrating systems over in order to reduce the amount downtime.	AWS suffers a DDOS attack or goes down; ISP has an outage; AWS experiences interruptions to their internal network.	Acceptance – Accept that much of the control is with the ISP and CSP and trust them to provide the best reliability that they can. Risk transference – Create service level agreements (SLA) with the ISP and CSP in order to transfer some of the risk to them instead of the data center. Stakeholders may not be happy with network interruptions, but at least the data center would be compensated for it.	1%	The chances of a network interruption are low but have a massive impact on production. A service level agreement (SLA) made with the Navy customer could be compromised, resulting in a loss of revenue.	Risk transference – A lot of the control is in the hands of the internet service provider and the cloud service provider. Rather than trusting they will prevent network interruptions, we should be able to come to an agreement in which we will be compensated for lost revenue if that happens.
2	Latency	Network performance is going to rely on more factors than just internal infrastructure. Resources that are provided by AWS are shared, which could also affect latency.	AWS experiencing high levels of traffic; Internet traffic is particularly high; Distance to ISP or CSP is further than desirable.	Risk exploitation – The data center could take advantage of this risk in order to make performance greater. CSPs provide things such as auto-scaling, edge computing (close physical locations), and other cloud tools.	5%	Latency could be a part of the SLA, but even if it is not, it would have a negative impact on the customers, and reduce the number of customers willing to work with the data center.	Exploitation – While the risk of experiencing latency could be an issue, we find that there are many tools available to us that would not only prevent latency, but eliminate some of it.

				Risk transference – Latency could be detailed within a service level agreement with an ISP or with a CSP taking the weight of latency issues being lifted from the data center.			
3	Vendor Lock-In	When migrating, a cloud service provider (CSP) may require a contract be made in order to be competitive with other providers in the market. Once you are locked in, it may be too late to make changes.	After signing a contract with a CSP, a potentially better offer is found with a different CSP.	Avoidance – Avoiding a vendor that has lock-in features would give the data center more control. Acceptance – Accept that there may be some service providers that require a contract to enter a deal.	30%	The data center would not be able to take advantage of the better prices offered by the other CSP. Alternatively, we could be locked into a good price with the CSP, even if they raise prices for other customers.	Acceptance – Accept the risk and trust that the vendor will provide the best deals. This will require as much research as possible before entering a contract with the CSP.
4	Employee cloud training	Cloud computing is a relatively new concept and is growing fast in the information technology market. There will be a learning curve with the transfer to cloud, so getting employees up to speed may take too much money and hiring new cloud engineers	The migration occurs and the lack of training/knowledge on cloud infrastructure produces too much administrative overhead.	Sharing – Make a deal with a cloud training company or consultant to get support with training. Enhancement – Invest money into cloud training resources such as Percepio.	55%	Lack of training and knowledge on cloud infrastructure will result in more time and money invested than is suspected. This could lower revenue.	Enhancement – Not all employees will need training on cloud infrastructure, so investing in some resources for employees to use in their free time

		may not be feasible financially either.					will save money over a consultant.
5	Production downtime	Migrating servers from on premise to cloud will require that production servers be taken offline until the new cloud server can be brought online. Careful planning will be necessary to minimize the amount of downtime.	A roadblock is encountered during the migration period.	Mitigation – Implement mechanisms and plans for reducing as much downtime as possible. Example: Properly train employees, create an on-call roster, track down time, etc. Acceptance – Accept that there may be times when a production outage may go longer than expected.	40%	Downtime not only puts the SLA at risk, but also will impact the customer’s websites that they host, affecting their end users as well.	Mitigation – Creating mechanisms, migration times, training employees, and implementing an on-call roster are all part of normal operations at the data center and will help with mitigating unnecessary down time.
6	Compliance violations	Defense Information Security Agency (DISA) requires strict policies and protocols and policies to be implemented. Some of these may be more difficult to adhere to considering we a lot of the control is transferred to AWS and not the data center.	A vulnerability within a Security Technical Implementation Guide (STIG) is encountered and cannot be mitigated due to moving to a cloud solution.	Acceptance – Acknowledge that there may be challenges associated with compliance when migrating to a cloud solution. Accept the fact that sometimes it is not feasible to cover every single finding (vulnerability). Infrastructure and compliance often conflict with each other. Escalation – Raise the compliance issue to high level management for awareness. Compliance	20%	The risk of compliance violations varies depending on the severity of the vulnerability that is open, and the quantity of them. If an auditor has determined that the data center has too many violations that are severe, we could be denied access to DoD networks, potentially shutting down the entire data center operation.gf	Escalation – Upper management support is a key success to all projects, especially considering compliance has such a big impact. We will need to escalate this risk to get some of the more difficult vulnerabilities covered. Accepting that they may be uncovered is not an appropriate risk

				is extremely important and will require close attention from cloud team leadership and Cyber Project management in order to remain on the DoD network.			management strategy in this scenario.
7	Cost mismanagement	Server provisioning, optimization, and usage may be hard to estimate. The data center will need to be careful with cloud operations in order to make the migration financially viable.	Management miscalculates the cost of provisioning server(s)	Enhancement – leveraging optimization strategies, monitoring usage, and using other tools available from a CSP could help to save money rather than lose it. Acceptance – Accept that there is an inherent risk when working with a CSP, and that the business relations team is able to calculate and plan accordingly and efficiently.	20%	Miscalculating the cost of provisioning cloud systems for customer use could result in a loss of revenue.	Enhancement – Using the tools and strategies provided to us, the data center will be able to make informed decisions to possibly save money
8	Data security/privacy breach	Cloud solutions have different methods of implementing security and data privacy into their systems. Employees need to know these methods just as well, if not better than how they implement security on premise. Data security breaches can cost companies	Poor security practices; Misconfigured security settings; Human error	Transference – Transfer the risk of cyber security to the cloud service provider. Mitigation – Implement policies, procedures, and mechanisms for controlling our own cyber security in order	45%	The average cost of a data breach in the United States is around 10 million dollars; Stakeholder trust will be lost; Possible denial of access to DoD networks; leaks of controlled unclassified information, NNPI, PII, and trade secrets.	Transference - 45% of companies in the US have been a victim of a data breach. With such a high probability and a high impact on the company, it is best to implement our

Your Name: Nathan Rickett
Risk Identification Exercise

		millions of dollars in damages and reparations.		to mitigate the risk of a data security/privacy breach.			own security controls rather than transferring that risk and relying on the CSP to do it for us.
--	--	---	--	---	--	--	--