ORM DEPLOYMENT RISK

Tyler O’Riley

CSD370 Assignment 11.2

10/09/2023

AMAZON DEPLOYMENT RISK MITIGATION: [Source](https://docs.aws.amazon.com/wellarchitected/latest/operational-excellence-pillar/mitigate-deployment-risks.html)

Amazon company has a structure called Operational Excellence Pillar which covers a comprehensive look at their operational risk management. On the topic of deployment risk, they have four primary practices they follow; Plan for unsuccessful changes, Test deployments, employ safe deployment strategies, and Automate testing and rollback.

Plan For Unsuccessful Changes

The first practice is to plan for a failed state. The simplest solution to a failed rollout is to simply prepare a rollback protocol to a previous version. The reason for this solution is to ensure a new update cannot deprecate the structure of a system. If the rollout occurs and an error happens, trying to come up with a fix/rollback post update can be a difficult endeavor. If the rollback is generated before the update is rolled out, it can be a quick and easy remediation process.

Test Deployment

Test Deployments are the next step to be taken in place of rollbacks. Obviously, a company does not want to expect a rollback to be needed and one way to avoid this is Testing the deployment. This step is like what we have learned in creating a parallel environment where a copy of the system can be tested without affecting the main system.

Employ Safe Deployment Strategies

This delivery method is to avoid impacts on the customer experience. A rollout can cause impacts on the system and a company’s goal is to make updates in a way so that even if an error occurs, the errors don’t affect the end user experience. In this strategy, post rollout errors are handled in priority of which errors are influencing the end users.

Automate Testing and Rollback

As the name implies, this strategy takes the first two practices and combines them into an automated practice. The reason you would seek to automate them is to assist with faster response times. If an automated rollback tool can catch an error as it happens, the response can be so fast that your end users would not notice the error occurred.

AUDITBOARD ORM PROCESS: [Source](https://www.auditboard.com/blog/operational-risk-management/)

Unlike Amazon where each practice is standalone, Auditboard approaches the topic in a four-step process called Risk appetite. The end goal is to evaluate your potential risks with any practice you use and decide if it will work best for deployment. The four steps include Risk Identification, Risk Assessment, Risk Mitigation, and Risk Monitoring. This method can be applied to amazons’ practices as an example.

Let’s say you choose to use test deployments as your primary practice. You should first identify the risks of this practice. You may not know how the update affects end users since this test is being conducted in a simulated environment. You would then assess this risk. How intense could the impacts be? Are these acceptable risks or would they have a negative impact? Once you have identified what is acceptable and what is not, you will work towards mitigating the unacceptable hazards. Finally, continuous risk monitoring must be conducted to keep track of all hazards post update.

INVESTOPEDIA: [Source](https://www.investopedia.com/terms/o/operational_risk.asp)

This source’s approach to risk assessment takes a holistic approach to internal, user, and external risk. Incorporating techniques from the other two sources I mentioned, Investopedia not only looks at the internal and end user experience but considers other risk factors. What if a new update leaves a gap in your system for someone trying to hack into your databases? What if the update leaves gaps for malware to be introduced to the system? These are the additional risks that they take into consideration among the other practices and factors that Amazon and Auditboard consider as well.

Out of these three resources, I would not recommend an individual one, rather all three bring great ideas to the conversation that should be considered. There is an infinite amount of risk that is impossible to keep track of them all. Using a combination of these three resources can at the very least help create a system where you can respond to levels of risk and be prepared to either remediate or roll back your deployments.