Risk managments strategy of applaying open stack system

Technology, Information Technology

Full Paper Open Stack Risk Management As of today, risk management can be considered as an old terminology that is being practiced by finance managers on almost all business models. Likewise, definition of risk varies from one domain to another. Similarly, IT managers conducting risk assessment does not have high risk ratings when compared to financial risks assessment. The definition of risk for IT professionals can be a probability or magnitude that may indicate loss in future. In spite of high flexibility options, and cost effectiveness, Open stack is not just an application. It is in fact an open source cloud computing solution that is built on precise components such as storage and network components that are integrated with each other to make a complete open source cloud computing solution. Accordingly, the source code is shared with the vendors as well as the development team. Consequently, the usability of Open stack can lead to unpredictable risks. Organization try to mitigate the risks associated with this unpredictable environment may create new risks by exposing the cloud on the Internet instead of utilizing an industry compliant standardized solution. The complex customization and flexibility of opens tack that can be specific to an organization may lead to a conflict with the external open stack infrastructure. Therefore, the internal and external semantics of the cloud infrastructure is hybrid (Mears, J. 2007).

Likewise, there is a risk of implementing changes on the open stack without performing impact analysis due to informal change management process. For instance, a patch needs to be deployed on the open stack and testing is required before implementation. The IT department will test the patch and attach the results in the change management form with formal approvals.

After the approvals, the patch can be deployed only if the test results are all correct. Similarly, patch management for open stack can also lead to vulnerabilities that can be exploited any time. For mitigation, effective patch management process needs to be in place for testing and applying patched in the production environment. The same change management process can be adopted for patch management. However for tracking end of life and end of service for information technology assets, an asset register is require for keeping track. Ideally, an IT asset coordinator is a key person who performs these tasks (KLEPS 2015).

After establishing an asset register, all the assets are now identified and ready for risk assessment. In the first step, the confidentiality, integrity and availability score will be added together. The risks assessment will further be carried out on a worksheet with the calculation of risk impact, probability, exposure and the output will be risk rating along with the risk owner. Moreover, the risks can then be mitigated by implementing controls, contingency plans and any additional risk strategies. The strategy for effective risk management for an organization utilizing open stack can be based on ISO/IEC 27001. The standard will not only enforce to put controls but will also make all the effective information security practices part of the process.

References

Mears, J. (2007). 4 Open source: Moving on up the stack. (cover story). Network World, 24(2), 30.

KLEPS, K. (2015). STACK EVOLVES, EXPANDS. Crains Cleveland Business, 36(8), 5-26.