Software Development Life Cycle for Data in Cloud Computing Environment

Chimene Tchokoko Diboma

School or Institution Name (University at Place or Town, State)

**Software Development Life Cycle for Data in Cloud Computing Environment**

**Operations and Maintenance:**

The client has to manage human resource applications in the cloud environment. As the implementation includes software as a service offering, the operations and maintenance support will be provided by the vendor as per the subscription agreement between the vendor and the client. Installed system and applications in a cloud environment require appropriate management services. Client-side applications will work without any further maintenance requirements, but the infrastructure operations will be monitored by the vendor to ensure the quality of service. During the term of the service agreement between the parties, the vendor will provide operations and management support for the project as per the following plan.

A team of professionals will be available to monitor the operations of the applications in managed infrastructure. The vendor will release application updates to address security holes in previously released application versions. However, no major change in architecture will be made to avoid compatibility issues with legacy applications of the client. Data related to human resource management applications contain personally identifiable information and integrity of the data in transit will be monitored by the dedicated teams (Weber, Nepal, & Zhu, 2016). The vendor will respond to and disclose any discovered anomalies in traffic patterns to the client. The reporting will be transparent and will engage the in-house information technology teams of the client as well. A telephone number will be made available to the client to contact the vendor in case of a support case covered by the service level agreement.

Email support will always be available to the client and client will be able to request support for covered applications. The support will not be provided for legacy applications developed by the client itself. Related documentation and reports of any possible issues or service downtime reports will be provided via email. Incident response teams of the vendor will be available 24/7. However, the recovery support or incident response will be provided as per the severity of the support ticket opened by the client. Severity level 1 will be reserved for the issues that produce emergency conditions. In case of a severity level 1 issue, the client must contact the vendor via phone line as compared to the email requests (Aljawarneh, Alawneh, & Jaradat, 2017). After receiving a severity level 1 support request the vendor will provide professional remediation support. In case of severity level, 2 or 3 support event or issues that do not directly affect the operation of the client can be requested by any of the available support channels.

Maintenance of internal infrastructure of the vendor will be scheduled on a monthly basis and the client will be informed well before time. However, any scheduled maintenance will not cause any disruption to the operations of the applications running in the cloud. The clients will be informed to mitigate any discrepancies if there is an outage caused by the maintenance for a fraction of time (Hehenberger et al., 2016). High availability access to the infrastructure will be maintained by the operations monitoring teams. Maintenance updates to the applications will be provided on a fortnightly basis. Research and development staff will install the updates and the updates will be tested for compatibility issues before the implementation of the patch.

Audit of the security systems is inevitable especially for mission-critical applications such as human resource management systems running in cloud environments. To ensure the confidentiality, availability, and integrity of data being transmitted to the cloud infrastructure, regular audits will be performed. Audits will be performed on a monthly basis and detailed audit reports will be shared with e client as well to ensure transparency of the systems. The vendor will schedule third-party independent audits of internal infrastructure and critical systems that will help in the understanding of the issues. Audits of the infrastructure related to the particular client as in this case will be performed by the in-house security engineers. Security engineers will access all of the logs and monitoring systems to detect anomalies in the traffic patterns. Auditing teams will test all of the parts of the infrastructure including client-side applications for security holes. All of the application programming interfaces will be checked for possible security loopholes (Kashfi, 2017). Penetration testing tools will be utilized such as packet captures, TCP dumps and man in the middle (MITM) techniques to check for the efficacy of security measures. They will try to compromise or breach the system by using all possible attack vectors. As a result of the efforts, a comprehensive audit report will be generated and provided to the client as well.

If there are any vulnerabilities or possible security breaches such as anomalies in traffic patterns detected, then the vendor will fix discovered issues as soon as reliably possible. Updates will be released to address the security issues indicated in auditing reports. Software updates will include bug fixes and security patches. However, software updates released by the vendor may not include new features to the applications. Any new features developed for the applications may be sold to the clients as add-on services if they require their functionality in their business operations (Ferry et al., 2018). As the security audits are planned to be run at the beginning of each month, any security issues discovered will be patched within one month or before the next scheduled audit. When a fix for possible security issues is released neither the vendor nor the client will delay the installation of the security patch to ensure the smooth running of the applications.

Dedicated teams will monitor the functionality of the system to ensure that day to day functionality of applications remains stable. Operations and maintenance team of the vendor will administer the directories used by the client and user access security as well. The client can request specific restrictions for certain users to ensure the confidentiality of information. Appropriate segregation between critical applications will be provided by the operations and management teams as well. Security engineers may try to integrate more and more features found in the client-side applications into their offerings to increase the efficiency of the subscription models of software as a service cloud offering (Rosa, 2018). It will be ensured that data transmission is secured with end to end encryption and the vendor cannot access data of the client. Encryption keys will be stored locally in client-side machines and will never be retrieved by the vendor. Even the emergency recovery keys will be stored in local systems or provided to the client in protected media to ensure that the vendor will never be able to break the encryption mechanism in any way. These measures must be practiced by the operations and maintenance teams of the vendor to maintain the trust of clients in their services.

**Disposal Plan:**

As the project will enter the finalizing stage, the project deliverables will be handed to the owner as per the disposal plan. At the final stage of implementation, all of the software installations and integrations will be verified and tested for appropriate functioning. Any performance flaws and functionality issues will be rectified. Along with the rectification of issues, their documentation will also be completed for future reference. Documentation of such issues and rectification steps will help the client to look for the solution of possible problems in the future without requiring direct support from the vendor. The design documents and specifications of the projects will be compiled into end user guides. Extra documents or paperwork related to the project will be disposed of appropriately.

Military grade shredding techniques will be utilized both for digital and paper-based information material. It is inevitable to use secure methods of disposal of critical information as a breach of such information can cause irreparable damage to both the vendor and the client as well. Digital information related to the internal infrastructure and applications will be encrypted using AES-256 bits encryption algorithm if it is required by the client. Otherwise, it will be shredded and discarded as the vendor do not require access to such information because all of the necessary details will be provided to the client via documentation of the project (Rittinghouse & Ransome, 2017). All the liabilities will be cleared. Accounts related to the project will be closed and all of the transaction receipts will be made part of the documentation related to future audits of the project costs. Employees of the client will be trained to use the newly installed systems. The training will cover the essentials of the project and will be based on the original agreement between the parties. As per the disposal plan, the vendor will never disclose information about the applications and security measures to any third parties. User manuals and troubleshooting guides of the equipment purchased from third parties will be handed over to the client.

**References**

Aljawarneh, S. A., Alawneh, A., & Jaradat, R. (2017). Cloud security engineering: Early stages of SDLC. *Future Generation Computer Systems*, *74*, 385–392.

Ferry, N., Solberg, A., Song, H., Lavirotte, S., Tigli, J.-Y., Winter, T., … Aguirre, A. C. (2018). ENACT Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems. *International Workshop on Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment*, 112–127. Springer.

Hehenberger, P., Vogel-Heuser, B., Bradley, D., Eynard, B., Tomiyama, T., & Achiche, S. (2016). Design, modeling, simulation and integration of cyber physical systems: Methods and applications. *Computers in Industry*, *82*, 273–289.

Kashfi, H. (2017). *Software Engineering Challenges in Cloud Environment: Software Development Lifecycle Perspective*.

Rittinghouse, J. W., & Ransome, J. F. (2017). *Cloud computing: implementation, management, and security*. CRC press.

Rosa, F. (2018). *Analysis of requirements and technologies to migrate software development to the PaaS model*.

Weber, I., Nepal, S., & Zhu, L. (2016). Developing dependable and secure cloud applications. *IEEE Internet Computing*, *20*(3), 74–79.