ISSN No:-2456-2165

Development of a Risk Management Framework for Software as a Service Provider

Rachelle De Los Santos
School of Computing
Graduate School of Holy Angel University
Philippines

Abstract:- The adoption of Software as a Service (SaaS) is becoming prevalent. With its ease of use and cost savings in time and management, many customers are shifting to usage of third- party applications to help them streamline and manage their business processes efficiently and effectively. SaaS providers must ensure that customer data is secure. To effectively manage the risks surrounding SaaS provider's IT infrastructure, a risk management framework was developed to identify, mitigate and evaluate potential impact of risks. This framework provided visibility into infrastructure security risks. It mapped the infrastructure of SaaS provider in compliance with ISO 31000:2018 and NIST Cyber security Framework. The risk management framework helped the SaaS provider better understand the security risks surrounding its SaaS solution. It also helped in the secure deployment of SaaS projects to drive improved user experience and high customer satisfaction. The gap assessment showed the areas where improvement must be made. Additional scenarios and continuous monitoring are needed to avoid a false sense of security.

Keywords:- *SaaS; risk management framework; security controls.*

I. INTRODUCTION

Software as a Service is the service provided by the software vendor to the customers where the software may reside in the provider's on-premise server or on the cloud provided by a third-party vendor. This service model is cost-efficient for the customer because SaaS pricing model is flexible. SaaS customers pay on subscription variations to suit their needs. SaaS providers may give a free trial period to allow customers to explore the application before deciding to subscribe.

The customer may choose to upgrade or downgrade the subscription depending on a number of factors. This may include business expansion, reduction in number of branches, increase or decrease of number of users and the need for advanced features. The customers achieve greater productivity while spending less.

Managing the customer data, the Software as a Service provider must identify security risks in its IT infrastructure and mitigate them to ensure that the data is secure.

Software companies can choose to build their applications on their own on-premise server or on the cloud to leverage their resources and produce high-yield opportunities. SaaS multi tenancy architecture allows the use of single database to be shared among tenants (SaaS customers). This reduces the cost of handling multiple databases. Multi tenancy scales to accommodate multiple customers without having to modify the database configuration. The customers are abstracted from accessing each other's data. A customer can only access the data relevant to him. SaaS providers use templates to enable reuse of configuration components to be deployed across multiple customers. SaaS providers perform the updates for all the customers simultaneously. This ensures that all customers are working on the latest version of the SaaS solution.

SaaS applications provide access to data anytime and anywhere to its customers through the internet unlike the traditional on-premise applications that limit accessibility. Customers shift to SaaS to reduce the overall cost of providing and maintaining their on-premise applications. There is no need for installation and software updates on the customer side. Hardware components like servers are not needed on the customer side, therefore eliminating the cost of maintenance and the need for internal IT personnel.

Security and privacy issues arise with the use of SaaS model. The security challenges are the confidentiality, integrity, and availability of customer data, network security, and application security.

This paper focuses on the development of a risk management framework and monitoring solution. Using ISO 31000:2018 Risk Management Framework and National Institute of Standards and Technology Cybersecurity Framework, the risks are identified for on-premise IT infrastructure design of SaaS provider, risk mitigation strategy is developed and recommended solutions to the security challenges are provided.

The customer does not know how the SaaS provider secure his data. The customer depends on the provider for the confidentiality, integrity, and availability of his data. Therefore, the SaaS provider should be proactive in managing the security risks surrounding its own IT infrastructure.

According to Gartner (2018), SaaS will grow to 17.8% in revenue in 2019 amounting to $85.1 billion. SaaS providers seek to help customers manage their information and business processes in a reliable and secure manner. SaaS providers should ensure that their customers' data is secured while being processed, transmitted and stored. It is expected that the SaaS provider ensures the confidentiality, integrity and availability of their customers' data.

The challenge with SaaS is that IT infrastructure security risks are inevitable. Vulnerabilities may be present in the hardware, network and software of the SaaS provider. The

vulnerabilities can be exploited by attackers to compromise the IT infrastructure.

With the increasing number of customers integrating SaaS applications into their existing systems, SaaS providers must adopt a proactive approach in finding and mitigating security risks in order to prevent data breach, business disruption and loss of customer confidence. SaaS providers must gain a wide visibility into the expanding threat landscape that could bring adverse effects to their organization.

If security risks are ignored, SaaS providers will have to add resources to handle security incidents. It could also result to penalties in service level agreement with the customers if the systems are down for extended periods, or worst, customer attrition. Regulatory compliance issues may also arise resulting to fines depending on the severity of the security incident.

The objectives in this study are: (1) To be able to develop a risk management framework for the SaaS provider, (2) To be able to recommend controls, show the residual risks, and treat the residual risks, (3) To be able to show the gaps between the current and target state in the IT infrastructure design of the SaaS provider, (4) To be able to determine the cyber security posture of the SaaS provider based on IS0 31000:2018 and NIST Cyber security Framework.

II. METHODOLOGY

This capstone project used both qualitative and quantitative research methodology. According to the article written by Dr. Stump fegger, qualitative research focuses on the data collected through interviews which will provide more insight into the subject matter being discussed while a quantitative research uses numbers to analyze and conclude on a specific research subject.

Research questions were given to the SaaS provider to gain a holistic view on their risk management practices. Research questions were about the SaaS infrastructure security risks, how they managed the risks, and the platform that they used for managing infrastructure security risks, if any. The SaaS provider answered the gap assessment to determine the current and target state of their hardware, software and network.

The conceptual risk management framework was used as a guide performing risk management and assessing the current cybersecurity posture of the SaaS provider. Risk assessment was performed for hardware, software and network. At the end of the risk assessment process, the SaaS provider was given the risk treatment option to treat the risk.

The current and target state was mapped to determine the gaps that were needed to fill to secure the IT infrastructure of the SaaS provider. The framework determined the controls that were not implemented that contributed to the system being unsecure.

The IT infrastructure was divided into 3 categories to easily identify where most risks came from. The categories used were hardware, software and network. The controls in each category were assessed by the SaaS provider. The result of the gap assessment could be low, medium or high which indicated the cybersecurity posture of the SaaS provider. The metrics are explained in the research instruments part.

The risk management and mitigation process were based on ISO 31000:2018 and NIST Cybersecurity Framework. The likelihood and impact of the risk scenarios were determined to be able to know the inherent risks on the SaaS provider's hardware, software and network infrastructure components. Controls were recommended to mitigate the inherent risks. The residual risk for the risk scenario was calculated after applying the recommended controls. The risk treatment options were provided to treat the residual risks.

The gap assessment showed the SaaS provider's current and target state in cyber security posture. It showed the controls that were implemented and the controls that were recommended to implement to further secure the SaaS provider's infrastructure.

III. RESULTS

A. Framework

Risk management is an iterative process that can be applied to the use of technology to be able to secure the IT infrastructure effectively. The risk management framework was developed based on the need to assess and mitigate the hardware, software and network risks. The components of the framework are Identify Risk, Assess Risk, Control Risk and Review Risk. The identification and assessment of risk were based on ISO 31000:2018. During the risk identification process, the risk scenarios related to hardware, software and network were identified. After establishing the risk scenarios, the risks were assessed based on their likelihood to happen and the impact to the organization if they happen. The control and review of risk components were based on NIST Cyber security Framework. The controls were established to minimize the risks. The risks were reviewed in order to determine if the controls were enough to minimize the risks or additional controls should be added.

The risk management process is the application of the framework. It describes how to perform risk identification, assessment, control and review. The components of the risk management process are Establish Context, Risk Category, Risk Identification, Risk Measurement, Risk Mitigation and Risk Treatment. The study utilized this process to be able to determine the risks, minimize the negative impact to the SaaS provider and keep the risks under control.

B. Risk Assessment

Establish Context

To be able to oversee cyber security risks, an understanding on the way the organization works must be developed. By understanding the context in which the business operates, the resources and the related risks allow the organization to prioritize its efforts in aligning risk management with the business needs. IT infrastructure and business environment of the SaaS provider are identified.

- Risk Category

Risk category is the grouping of risks. The risk categories in this research project are hardware, software and network.

- Risk Identification

Risks are identified based on the establishment of context and risk category. The risk scenarios are established for hardware, software and network of the SaaS provider.

- Risk Measurement

Risks are measured based on the likelihood that a threat will exploit avulnerability in the hardware, software and network of the SaaS provider. The impact of such likelihood is determined to be able to calculate the inherent risk.

To determine what the likelihood is for a certain risk scenario, the user was guided by the likelihood definition and rating for better assessment. The risk scenario has a likelihood of 'rare' with '1' as rating when the scenario happens under exceptional condition. The risk scenario has a likelihood of 'unlikely' with '2' as rating when the scenario is not likely to happen in common condition. The risk scenario has a likelihood of 'possible' with '3' as rating when the scenario is possible to happen under any condition. The risk scenario has a likelihood of 'likely' with '4' as rating when the scenario is likely to happen in most conditions. The risk scenario has a likelihood of 'almost certain' with '5' as rating when the scenario is expected to happen in most conditions.

To determine what the impact is for a certain risk scenario, the user was guided by the impact definition to better assess the risk. The risk scenario has an impact of 'insignificant' with '1' as rating when the negative impact has no effect to the business. The risk scenario has an impact of 'minor' with '2' as rating when it has a slight negative impact to the business but without disruption. The risk scenario has an impact of 'moderate' with '3' as rating when it has a moderate negative impact and cost increase to the business. The risk scenario has an impact of 'major' with '4' as rating when it causes major damage and significant cost to the business. The risk scenario has an impact of 'catastrophic' with '5' as rating when there is a complete system failure and loss.

The inherent risk was determined given the likelihood and impact that were selected for a risk scenario. The inherent risk was calculated by multiplying the likelihood that a threat will exploit a vulnerability and the potential negative impact to the SaaS provider if the vulnerability is exploited successfully. The formula is Inherent Risk = Probability x Impact.

The risk score table shows the rating for the score obtained after calculating the inherent risk for a risk scenario. The score is converted to percentage. For minimum risk, the current controls are maintained. For low risks, the current controls are improved. For medium and high risks, additional controls are applied. For extreme risk, the activity is discontinued until the risk is reduced.

- Risk Mitigation

Recommended controls were provided to mitigate the inherent risks. The recommended controls were rated based on its effectivity to reduce the inherent risk. The control is not effective if the inherent risk is not reduced. The control is weak if the inherent risk is reduced by 30%. The control is moderate if the inherent risk is reduced by 50%. The control is strong if the inherent risk is reduced by 90%.

- Risk Treatment

Residual risk is the remaining risk after a control is applied to inherent risk. The residual risk is calculated by inherent risk value minus the control, Residual Risk = Inherent risk - Control.

The risk assessment result summary demonstrated that the SaaS provider had a residual risk of 13% for hardware, 62% for software and 25% for network. Residual risks are treated by avoidance, acceptance, transfer and reduction. Risk Avoidance is when the activity that has a high risk is avoided and discontinued. Risk Acceptance is when the activity that has a low risk or the risk is easy to manage is accepted and no further action is required. Risk Transfer is when the risk of an activity is transferred to a third party like insurance company. Risk Reduction is when the risk of an activity is reduced by adding controls. The SaaS provider accepted risk scenarios that had a residual risk of 20% that cannot be further reduced by recommended controls. The SaaS provider didn't transfer nor avoided risks.

The hardware residual risks were reduced by 82% after applying the recommended controls. The remaining residual risk of 18% was accepted.

The software residual risks were reduced by 50% after applying the recommended controls. The remaining residual risk of 50% was accepted.

The network residual risks were reduced by 88% after applying the recommended controls. The remaining residual risk of 12% was accepted.

C. Gap Assessment

The gap assessment determined the gaps between the current and the target state of the SaaS provider. The gap assessment is divided into three categories namely: hardware, software, and network.

The SaaS provider had security controls in place for 9 activities related to hardware. The target was to have security controls for all 11 hardware activities that were specified in the risk scenario. Hardware had a gap of 18%. The first gap was the use of removable media is not controlled on information system components. The second gap was the use of portable storage devices that have no identifiable owner are not prohibited. Recommended controls were provided to address the gaps in hardware. To address the first gap which was "the use of removable media is not controlled on information system components", the control was to "prohibit the use of portable storage devices in information systems when such devices have no identifiable owner ". To address the second gap which was "the use of portable storage devices that have no identifiable owner are not prohibited", three controls were recommended. The controls were "block all USB media except the ones you purchased", label keys before issuance", and "track issued keys in your inventory".

The SaaS provider had security controls in place for 11 activities related to software. The target was to have security

controls for all 12 software activities that were specified in the risk scenario. The software had a gap of 8%. The gap was that the user-installed software was not controlled and monitored. The recommended control was provided to address the gap in software. To address the gap which was "User-installed software is not controlled and monitored", the control was "user controls will be in place to prohibit the installation of unauthorized software. All software for information systems must be approved".

The SaaS provider had security controls in place for 31 activities related to network. The target was to have security controls for all 32 network activities that were specified in the risk scenario. The network had a gap of 3%. The gap was that the connection of mobile devices to the network is not controlled. Recommended control was provided to address the gap in network. To address the gap which was the "connection of mobile devices to the network is not controlled.", three controls were recommended. The controls were "The organization establishes usage restrictions, configuration requirements, connection requirements, Implement guidance for organization-controlled mobile devices and Authorize the connection of mobile devices to the information system".

D. Cyber security Posture

Likert scale was used to evaluate the gaps. Yes is given the value of 1 and No is given the value of 0. The value of yes was calculated to get the mean. If the mean is low, which is between 1 to 6, it has a high risk and needs improvement to protect IT infrastructure. If the mean is medium, which is between 7 to 12, it has average risk and needs further improvement. If the mean is high, which is between 13 to 18, it has a high defense against known threats to risk scenarios but continuous monitoring and assessment is needed.

The mean of the scores is 17 and based on the likert scale for cyber security posture in this context, the SaaS provider had a high defense against known threats to risk scenarios but continuous monitoring and assessment is needed since the list of risk scenarios is not exhaustive.

IV. CONCLUSION

The adoption of Software as a Service is growing because of its fast deployment and ease of use. The customer can spend more time focusing on their business and less time building the infrastructure. To gain customer confidence, the SaaS provider must ensure that their infrastructure and the customer data are secure. The development of risk management framework helped the SaaS provider better manage the risks surrounding their infrastructure.

This research developed a risk management framework for the SaaS provider to be able to show the inherent risks, recommend controls to mitigate the risks and treat the residual risks. Risk scenarios for hardware, software and network were identified to be able to analyze and assess the risks properly. The current state was compared to the target state to be able to identify the gaps. This comparison showed the state the SaaS provider was in and the desired state where the SaaS provider would want to be. Controls were recommended to minimize the gap.

The framework simplified the process of assessing and mitigating risks. Keep in mind that the list of risk scenarios was not exhaustive and that updating it will provide a full coverage of the risk scenarios related to the IT infrastructure of the SaaS provider.

REFERENCES

[1.] Adi, P. (2015). *Scrum Method Implementation in a Software Development Project Management*. Retrieved from Research Gate: https://www.researchgate.net/publication/283435871_Scrum_Method_Implementation_in_ a_Software_Development_Project_Management

[2.] Araujo, V., & Vázquez, J. (2013). Business and Technical Requirements of Software-as-a- Service: Implications in Portuguese Enterprise Business Context. Retrieved from Cornell University: https://arxiv.org/ftp/arxiv/papers/1312/1312.2243.pdf

[3.] Bemrose, B. (2014). *Implementing and Integrating SaaS Solutions at Small Businesses.* Retrieved from CiteSeerX: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1006.8466&rep=rep1&type=pdf

[4.] British Standard. (2018). Risk Management - Guidelines. Retrieved from: https://www.ashnasecure.com/uploads/standards/BS%20ISO%2031000-2018.pdf

[5.] Buchanan, B. (2015). *Swimming in molasses... days of salting a password may be passing.* Retrieved from The Cyber Academy PBKDF2 LinkedIn: https://www.linkedin.com/pulse/swimming-molases - days-salting-password-may-passing-william-buchanan

[6.] Cisco. (n.d.). *Software-Defined Networking.* Retrieved from Cisco: https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html#~stickynav=4

[7.] Dinh, H., Lee, C., Niyato, D., & Wang, P. (2011). *A survey of mobile cloud computing:* architecture, applications, and approaches. Retrieved from Wiley: https://onlinelibrary.wiley.com/doi/full/10.1002/wcm.1203

[8.] Gartner. (2018). Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent *in 2019.* Retrieved from Gartner: https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17- percent-in-2019

[9.] Hurtaud, S., & Vaissière, L. (2014). *How to ensure control and security when moving to SaaS/cloud applications*. Retrieved from Deloitte: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu_ensure-control-security-saas-cloud- applications_07102014.pdf

[10.] Infosec. (2018). Risk Treatment Options, Planning and Prevention. Retrieved from Infosec Institute: https://resources.infosecinstitute.com/risk-treatment-options -planning-prevention/#gref

[11.] IRM. (2018). A Risk Practitioners Guide to ISO 31000:2018. Retrieved from Institute of Risk Management: https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf

[12.] Kolomiyets, T. (2017). Guidelines on Risk Management. Retrieved from UNECE: https://statswiki.unece.org/display/GORM/2.1+Establishing+the+context
[13.] Lachapelle, E., Aliu, F., & Emini, E. (2018). *ISO 31000 :2018-Risk Management Guidelines.* Retrieved from PECB: https://pecb.com/whitepaper/iso-310002018-risk-management-guidelines
[14.] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/ Legacy/SP/nistspecialpublication800-145.pdf
[15.] NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.Gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[16.] Nohe, P. (2019). How to Perform a Cyber Risk Assessment. Retrieved from Hashedout: https://www.thesslstore.com/blog/cyber-risk-assessment/
[17.] Oracle. (2012). *Cloud Reference Architecture.* Retrieved from Oracle: https://www.oracle.com/technetwork/topics/entarch/oracle-wp-cloud-ref-arch-1883533.pdf
[18.] OWASP. (2017). OWASP Top 10 – 2017 The Ten Most Critical Web Application Security *Risks*. Retrieved from Open Web Application Security Project: https://www.owasp. org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
[19.] Panetta, K. (2018). *Is the Cloud Secure?* Retrieved from Gartner: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
[20.] Praxiom. (n.d.). ISO 31000 2018 Plain English Definitions. Retrieved from Praxiom Research Group Limited: https://www.praxiom.com/iso-31000-terms.htm#Context
[21.] Ramalingan, R. (2017). IT Security Management and Risk Assessment. Retrieved from Slideshare: https://fr.slideshare.net/RajasekarVr/it-security-management- and-risk-assessment
[22.] Rane, P. (2010). Securing SaaS Applications: A Cloud Security Perspective for Application *Providers*. Retrieved from Information Security Today: http://www.infosectoday.com/Articles/Securing_SaaS_Applications.htm
[23.] Rashmi, Sahoo, G., & Mehfuz, S. (2013). Securing Software as a Service Model of Cloud *Computing: Issues and Solutions.* Retrieved from Cornell University: https://arxiv.org /ftp/arxiv/papers/1309/1309.2426.pdf
[24.] Rass, S. (2017). On Game-Theoretic Risk Management (Part Three) - Modeling and *Applications.* Retrieved from Research Gate: https://www.researchgate.net/ /publication/320821063_On_Game-Theoretic_Risk_Management_Part_Three_Modeling_and_Applications
[25.] Sen, A., & Tiwari, P. (2017). *Security Issues and Solutions in Cloud Computing.* Retrieved from Semantics Scholar: https://pdfs.semanticscholar.org/f607/9f8a10f11389ff565487fe84996ce26dc7e9.pdf
[26.] Sen, J. (2013). Security and Privacy Issues in Cloud Computing. Retrieved from Cornell University: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf
[27.] Sharkasi, O. (2015). Addressing Cybersecurity Vulnerabilities. Retrieved from ISACA: https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/addressing -cybersecurity-vulnerabilities.aspx
[28.] Soofi, A., Khan, I., Talib, R., & Sarwar, U. (2014). *Security Issues in SaaS Delivery Model of Cloud Computing*. Retrieved from Academia: https://www.academia.edu/6306691/ Security_Issues_in_SaaS_Delivery_Model_of_Cloud_Computing_
[29.] Stumpfegger, E. (2017). Qualitative Versus Quantitative Research. Retrieved from Munich Business School: https://www.munich-business-school.de/insights/en/2017/ qualitative-vs-quantitative-research/
[30.] Subramanian, S., & Munuswamy, D. (2015). *Security Mysteries in the Cloud*. Retrieved From ISACA: https://www.isaca.org/Journal/archives/2015/Volume-3/Pages/security -mysteries-in-the-cloud.aspx
[31.] Suganya, V., & Shanthi A. (2015). Mobile Cloud Computing Perspectives and Challenges. Retrieved from International Journal of Innovative Research in Advanced Engineering: http://www.ijirae.com/volumes/Vol2/iss7/13.JYAE10113.pdf
[32.] Sutton, J., & Austin, Z. (2015). Qualitative Research: Data Collection, Analysis, and Management. Retrieved from US National Library of Medicine National Institutes Of Health: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4485510
[33.] Zongo, P. (2016). *Managing Cloud Risk: Top Considerations for Business Leaders.* Retrieved from ISACA: https://www.isaca.org/Journal/archives/2016/volume-4/Pages/managing-cloud-risk.aspx