Tupan Technologies, Inc.

Information Systems Security Plan (ISSP)

Daniel Cordeiro Marques

University of San Diego

CSOL-550-01-SU21 - Management and Cyber Security

Dr. Michelle Moore

June 26, 2021

Table of Contents

1: Company Summary

Tupan Technologies, Inc. ("TT") is a software engineering company offering a diversified portfolio to help clients with personal budgeting and financial education. Through its cloud-based platform "Cuca," TT allows its 50,000 clients to control their expenses and follow the progress of their investments. Due to the sensitive nature of the information handled by the Cuca platform, cybersecurity is the cornerstone of the company's operations. This Information Systems Security Plan (ISSP) specifies Cuca's security requirements and outlines the controls that satisfy them (Swanson et al., 2006) according to the recommendations provided by the NIST SP 800-18.

1.1 Enterprise Architecture

TT adopts a cloud-based architecture to offer its products and to support employee's daily activities, as follows:

Business applications. TT's business applications (such as email, customer relationship management (CRM), and code version control) use a Software as a Service (SaaS) model hosted by service providers.

Customer applications. Customer-facing applications leverage a combination of Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) to dynamically deploy test environments and quickly reflect changes in production.

TT maintains complete segmentation between business and customer applications, enforcing separation of duty through Identity and Access Management (IAM). Employees work remotely using company-provided equipment.

1.2 Information System Name/Title and System Categorization

This ISSP uses the FIPS 199 (National Institute of Standards and Technology, 2004) to categorize the system based on the potential impact an adverse event causes on a security objective. Cuca is a high-impact system, as demonstrated by Table 1.

Table 1. *Cuca Cloud Platform Security Categorization*

Information System Name: *Cuca Cloud Platform*			
Information Type	**Confidentiality impact**	**Integrity impact**	**Availability impact**
Personally Identifiable Information. The platform stores the date of birth, email, payment information, and phone number for all its users.	**HIGH** The impact of unauthorized disclosure of PII may include fines associated with privacy laws and loss of confidence from users.	**HIGH** Changing the user's email address might allow attackers to impersonate platform users and access sensitive information.	**LOW** Users might temporarily lose access to real-time data and statistics generated by the platform.
System Categorization	Overall system impact (based on the highest impact): **HIGH**		

1.3 Information System Owner & Authorizing Official

Table 2 lists the contact information for Cuca's System Owner and the Authorizing Official.

Table 2. *Cuca's System Owner and Authorizing Official contact information*

Information System Owner	**Authorizing Official**
John Doe - Cuca Lead Engineer Email: jdoe@tupantechnologies.com Phone: (555) 538-5490	Jack Bruce - CTO Email: jbruce@tupantechnologies.com Phone: (555) 538-5099

2: Management

2.1 Roles and Responsibilities

Chief Information Officer (CIO). The CIO is responsible for reviewing and approving the ISSP alignment with the company-wide security plan.

Chief Information Security Officer (CISO). The CISO is responsible for implementing and managing the ISSP and ensuring the effective application of security controls.

Chief Privacy Officer (CPO). As clients might reside in different states and countries, the CPO is responsible for reviewing the ISSP and ensuring compliance with relevant privacy regulations (Johnson, 2014, p. 42).

Information System Owner (ISO). The ISO serves as the primary point of contact for the system. They are responsible for supporting the development and maintenance of the ISSP and coordinating efforts with the development team to ensure its implementation (Swanson et al., 2006).

Authorizing Official (AO). The AO is responsible for approving the ISSP, allowing the system's operation, and accepting potential residual risks (Swanson et al., 2006).

2.2 Planning Management

The CISO should appoint a Program Manager (PM) to continuously monitor the ISSP implementation progress using standard project management practices. The PM, CISO, the ISO, the AO, the Information Technology (IT), and the development team must meet weekly to align expectations and correct any deviations in the implementation plan.

2.3 Implementation Management

The teams must follow a phased approach to ensure timely and effective implementation of controls through tests and acceptance procedures that verify quality and compatibility.

2.4 Risk Management

The CISO and the PM must ensure that risks to the project and the systems are handled according to the company's risk management policies. TT uses the NIST Risk Management Framework (RMF) to select, specify, implement, and monitor security controls (National Institute of Standards and Technology, 2016).

2.5 Human Resources Management

The CISO, with the ISO and AO support, is responsible for selecting and appointing qualified personnel to implement the ISSP. Team leaders will perform quarterly performance reviews of their direct reports, while the CISO and ISO will monitor the team leads performance. The Human Resources department will keep track and document the reviews performed every quarter. The CISO must also establish requirements for certification and training and define performance metrics applicable to the people implementing the security plan. These metrics must measure the success of the ISSP implementation. Finally, all personnel with privileged access to Cuca must go through a background check before being hired. TT must apply appropriate sanctions in case of confirmed deviations from the security policy.

2.6 Cost Management

The CISO and the CIO must determine an adequate budget according to the CT's risk appetite (Touhill & Touhill, 2014). The PM must continuously monitor the ISSP implementation

budget, ensuring that costs do not exceed the estimates without approval from the CISO and the CIO.

3: Planning

3.1 Information Security Implementation (Security Controls)

As a high-impact system, the Information System Owner must implement the following baseline security controls recommended by NIST SP 800-53 (National Institute of Standards and Technology, 2020) to safeguard customer data. The Information System Owner must document

3.1.1 Physical security. The cloud service provider (CSP) must ensure that physical access to the data center is controlled, monitored, and restricted only to authorized personnel. The CSP must ensure continuous review of the list of authorized personnel and frequently review access logs, alerts, and surveillance systems. Applicable NIST SP 800-53 controls: AU-6(6), PE-2, PE-3(1), PE-6(1), SR-2(1), SR-3(3), and SR-6.

3.1.2 Access control. Cuca must enforce a clear separation of duties between privileged and non-privileged accounts, such as customers and platform administrators. Customers must be constrained to their environment and should not access or modify information from other users. Additionally, Cuca's session management and access control practices must follow the recommendations outlined by Turpin et al. (2010, pp. 6-8). Finally, Cuca must offer multi-factor authentication to all users. Applicable NIST SP 800-53 controls: AC-1, AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(11), AC-2(12), AC-2(13), AC-3, AC-4(4), AC-5, AC-6(1), AC-6(2), AC-6(3), AC-6(5), AC-6(7), AC-6(9), AC-6(10), AC-7, AC-8, AC-10, AC-11(1), AC-12, AC-14, AC-17(1), and AC-17(2).

3.1.3 Website data security. Cuca must follow the secure development best practices such as those recommended by Turpin et al. (2010, p. 10). Furthermore, Cuca must encrypt sensitive data in transit, in use, and at rest. The website must force the use of encrypted communication between the user and the application. Applicable NIST SP 800-53 controls: AC-4(4), AC-17(2), AC-19(5), SC-8, SC-8(1), SC-12, SC-12(1), and SC-17.

3.1.4 Mobile and cloud service. The CISO must ensure all cloud providers comply with TT's security policies and the relevant laws and regulations. SaaS and PaaS providers must offer mechanisms to encrypt Cuca-related data according to TT's requirements. The Cuca mobile application must execute within a secure container and encrypt sensitive data in the user's device. Applicable NIST SP 800-53 controls: AC-19(5), PS-7, SA-9, and SA-9(2).

3.1.5 Timely integration of information. A centralized server must store Logs and other audit records in real-time. The centralized server must allow correlation and real-time alerts according to thresholds established by the application owner and TT's security monitoring guidance. Applicable NIST SP 800-53 controls: AU-1, AU-2, AU-3, AU-3(1), AU-4, AU-5, AU-5(1), AU-5(2), AU-6, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-7, AU-7(1), AU-8, AU-9, AU-9(2), AU-9(3), AU-9(4), AU-10, AU-11, AU-12, AU-12(1), and AU-12(3).

3.1.6 Reliable communication. Cuca must reliably deliver information to users. As such, fallback communication lines must be in place, such as the use of alternative cloud providers. Applicable NIST SP 800-53 controls: WIP.CP-8, CP-8(1), CP-8(2), and CP-8(3).

3.1.7 System development and maintenance. Cuca's development and maintenance life cycle must follow the processes outlined by NIST SP 800-160 (Ross et al., 2016), and the

System Owner must ensure that security in the development stages. Applicable NIST SP 800-53 controls: SA-3, SA-10, SA-11, SA-15, SA-15(3), SA-17, and SA-21.

3.2 Contingency Planning

The CISO and the System Owner must develop a Business Impact Analysis (BIA) to identify the potential outcomes of an adverse event against the Cuca platform (Swanson et al., 2010, p. 15). Based on the BIA, the CISO and the System Owner must develop Incident Response (IR) and Disaster Recovery (DR) Plans that address the steps necessary to respond and recover the Cuca to a functional and eventually fully operational state. The System Owner must test these plans annually to ensure their efficacy.

3.2.1 Natural calamities. Being a cloud-based platform offers flexibility to host Cuca's supporting servers in multiple geographic locations physically. The DR plan must include a recovery strategy that uses an alternative cloud provider with data centers in different cities and countries, including procedures to switch between providers. The location selection must consider the potential for natural disasters.

3.2.2 Power outage. The DR plan must include a recovery strategy using an alternative cloud provider like the recovery from natural calamities. The providers must provide their recovery plans for a power outage event. The AO must approve the providers' DR plan.

3.3 Business Continuity Plan (BCP)

Based on the BIA, the CISO and the System Owner must decide which functions are essential for Cuca's operations and the required resources to continue operating. The CISO must review and update TT's company-wide BCP to ensure it covers these requirements. The System

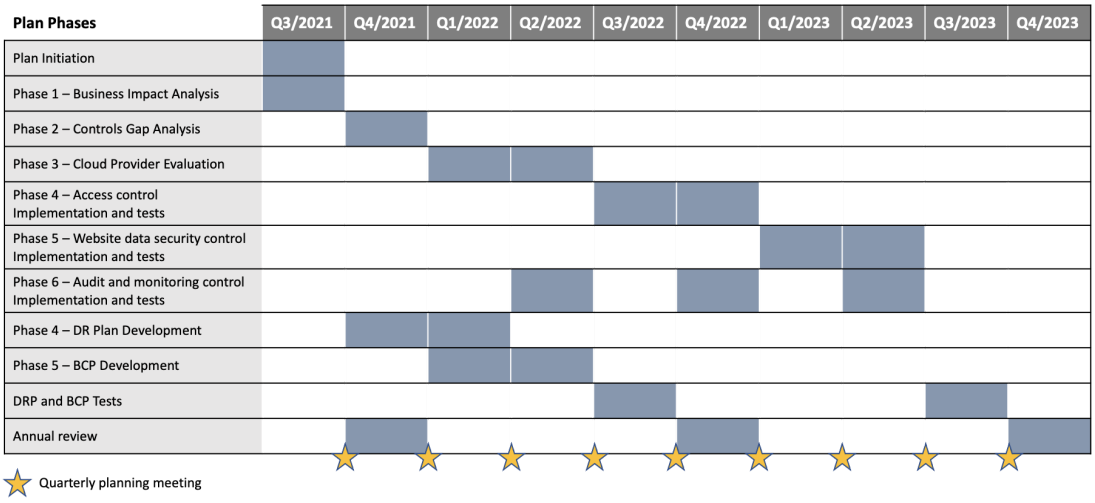
Owner must test the BCP annually to ensure its efficacy. Furthermore, TT is not under any regulatory obligations that might impact the business continuity strategy.

4: Implementation Management

4.1 Proposed Timeline/Execution

The plan will be executed in phases, with quarterly checkpoints to evaluate the progress and annual reviews to understand gaps, budgetary constraints, and personnel performance. After implementing each access and data security control, TT will start integrating continuous monitoring and audit logging controls to the centralized server. Figure 1 outlines the high-level timeline to execute the ISSP.

Figure 1. *The high-level execution plan for the ISSP*



4.2 Related Laws/Regulations/Policies

Cuca handles PII and payment information from customers primarily. The CPO must continuously review policies and procedures to ensure they comply with applicable privacy laws and standards.

4.2.1 Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS establishes requirements to manage and store payment information. For instance, Cuca must encrypt credit card details from its customers (PCI Security Standards Council, 2018).

4.2.2 Local Privacy Laws. As Cuca's users may reside in different states and countries, the CPO must also review the requirements for local privacy laws, such as the European Union General Data Protection Regulation (GDPR). If requirements significantly affect TT's bottom line, the CPO and the CEO may not offer the Cuca Platform Services in one or more locations.

5: Risk Management

TT must follow the NIST Risk Management Framework (RMF) to assess the potential cybersecurity risks affecting the Cuca platform (National Institute of Standards and Technology, 2016). The risk management activities are incremental, as the plan implementation and the platform operation might uncover new information that will help in fine-tuning the risk management process (MITRE, 2014). The CISO and the Information System Owner must document and communicate the risks to the senior leadership.

5.1 Risk Identification

The CISO and the Cuca's Information System Owner must perform a yearly review to identify threat sources and adverse events affecting the system (Joint Task Force, 2018, p. 41).

From an ISSP level, during the quarterly meetings, the CISO and the System Owner should review the plan's scope, dependencies, budget, performance indicators, and challenges (MITRE, 2014, p. 613).

5.2 Risk Assessment

Based on the information collected during the Risk Identification, the CISO and the Cuca's Information System Owner must classify threats and vulnerabilities and calculate the likelihood and potential impact of the adverse events materialize (Joint Task Force, 2018, p. 41). The risk assessment must consider risks associated with the Cloud Service Providers, including their impact on the business continuity and incident response process and procedures (Joint Task Force, 2018, p. 42). The categorization of threats, vulnerabilities, impact, and impact should follow the dispositions of NIST 800-30 Revision 1 (Joint Task Force, 2012, pp. E-1 - H-3).

5.3 Analysis & Prioritization

During the analysis phase, the CISO and the System Owner classify risks based on their probability and impact, according to the risk rating methodology provided by Joint Task Force (2012) and the annualized loss expectancy (ALE). TT's mitigation efforts must prioritize risks classified as "Very High" and "High." Section 5.5 offers additional details on the classification of risk.

5.4 Mitigation Planning, Implementation & Monitoring

The System Owner should create plans to address risks classified as "Very High" and "High" within six months of the risk assessment report issuance, and senior leadership must approve implementation costs. Once the System Owner implements these controls, the CISO must continually monitor their efficiency and take corrective actions when needed (MITRE, 2014).

5.5 Classification of Risk

From a semi-qualitative perspective, the CISO and the System Owner must classify the risk based on the combination of its probability and impact factors using a “Very Low” (negligible adverse effect on Cuca’s operation) to “Very High” (catastrophic consequences to Cuca’s operations) as recommended by Joint Task Force (2012, p. I-1 - I-2).

The CISO and the System Owner must also calculate the annualized loss expectancy (ALE) associated with each risk to complement the semi-qualitative analysis and create a threshold for required cybersecurity investments. As noted by Touhill & Touhill (2014, p. 58), The ALE takes into account the expected financial impact caused by the security objective’s loss (represented by the single loss expectancy - SLE) multiplied by how often the loss occurs in a year (annualized rate of occurrence, ARO).

5.6 Data-driven Risk

Cuca handles PII primarily from customers; therefore, data breaches offer great risk to TT. Whenever possible, the risk assessment should consider the data provided by industry research and the tools implemented to monitor security controls to understand the impact of a potential data breach and attacks targeting customer data.

5.7 Business-driven Risk

As the implementation of security controls must not impact Cuca’s time-to-market, the CISO and System Owner constantly review the ISSP implementation to ensure timely and efficient implementation of the plan. Furthermore, the ISSP is designed to support TT’s compliance and business continuity efforts.

5.8 Event-driven Risk

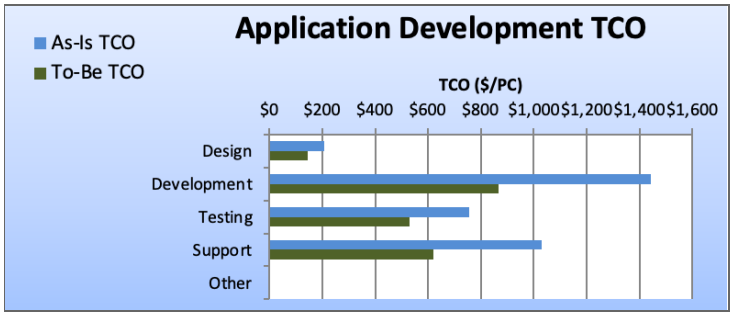
The CISO and the Security owner review this ISSP when an adverse event occurs to ensure accurate and effective control implementation. Lessons learned from the event (include those that impact the industry and not necessarily TT's operations) drive improvements and updates to the ISSP during the quarterly review.

6: Cost Management

6.1 Provide Security Infrastructure That Reduces Development Costs

Figure 2 illustrates how the PaaS model significantly reduces the development costs by providing automated source code tests against common vulnerabilities and secure storage of the source code.

Figure 2. *Total Cost of Ownership (TCO) savings*



6.2 Reduce Operational Costs

The cloud-based BCP and DRP also provide a significant reduction of operational costs. Since the TT operates completely remote, there are no requirements to send employees to a different location; additionally, the costs of maintaining a secondary physical data center are transferred to the cloud provider. Using the cold site strategy based on various cloud providers

that can activate servers on-demand in different geographical locations reduces infrastructure-related costs.

6.3 Costs of Security

The cost to implement controls that mitigate risks should not exceed their ALE. Based on Ponemon Institute (2020), a potential customer database breach can result in an ALE of $ 15 M; the expected budget to implement this ISSP is $ 10M.

6.4 Planned Costs

The following costs are planned to implement this ISSP:

6.4.1 Third-party consulting for the BIA, risk assessment, and gap analysis. TT will hire a third-party consulting firm to perform a BIA, a control gap analysis, and a risk assessment in the first quarter of the security plan. The estimated cost is $ 200,000.

6.4.2 Software acquisition. The estimated cost of software license purchases and implementation to implement the security controls is $ 200,000 per year.

6.4.3 Personnel. The estimated cost of personnel (including hours and hiring a specialized workforce) is $ 2M per year.

6.4.4 Cloud service providers. The estimated cost of contracting cloud service providers following the PaaS, SaaS, and IaaS models is $ 750,000 per year.

6.6 Potential Costs

Potential unexpected costs include personnel turnover, a surge in cloud provider prices, and unforeseen changes in privacy regulations that might require additional investments in security controls. If a breach occurs, TT might also be subject to regulatory fines.

6.7 Comparative Costs With Industry

Bernard & Nicholson (2020) suggests that companies in the same sector as TT spend approximately 0.8% of their revenue on Cybersecurity per year. Estimated costs represent 0.7% of the 2020 revenue, which positions TT close to the same spending as its competitors.

7: Analysis and Recommendation Management

7.1 Key Elements

The successful analysis of the plan must consider three aspects: the risk assessment output and the control implementation efficacy in addressing these risks, the planned budget in comparison of the actual spending, and the proposed timeline *versus* the implementation progress. The CISO must evaluate these aspects during the quarterly review and document recommendations to improve the implementation process. Next, the System Owner must coordinate with the relevant teams to address the recommendations. During the annual review of the plan, the CISO must revisit the recommendations and evaluate if their implementation mitigates potential risks.

7.2 Conclusion and Future Work

This ISSP follows the recommendations provided by the NIST SP 800-18 (Swanson et al., 2010) to outline the security controls that address the risks associated with the Cuca Platform operations. The work also provides an overview of an expected timeline to implement these controls and the associated costs. Moving forward, Tupan should consider performing a penetration test against the Cuca Platform, with the primary objective of testing how the implemented controls will stand against an attacker in a controlled manner.

8: Assessment of ISSP to Cyber Management

The Cuca Platform ISSP covers the main aspects of planning, implementation, risk, and cost management expected in similar plans. As stated in the ISSP, the platform primarily handles customer PII, exposing Tupan Technologies to significant risk if data gets exposed to external threats; the company might be subject to regulatory fines, loss of customer trust, and sanctions the PCI council if payment data is compromised. As such, the ISSP correctly classified Cuca as a High-impact system according to the FIPS 199 classification methodology (National Institute of Standards and Technology, 2004). Following that classification, selecting the high baseline offered by the NIST SP 800-53 (National Institute of Standards and Technology, 2020) was appropriate to address the risks outlined in the document. However, the CISO and the System Owner should consider describing clear risk statements and how the proposed controls handle them, as recommended by MITRE (2014).

The cost estimates are appropriate for the initiatives outlined by the ISSP. As noted by Schneier (2008), security investments must take into account their impact on the organization's bottom line; the costs associated with implementing the controls proposed in the ISSP represent less than 1% of the TT's revenue and offer savings in the long term that positively impact the company's profit.

Finally, Tupan Technologies should consider expanding the plan to include yearly penetration tests to evaluate control implementation and training covering executives and company user's supporting the Cuca Platform (such as the help desk) to ensure they understand potential cybersecurity risks and their role in maintaining the organization security policy (Touhill & Touhill, 2014).

References

Bernard, J., & Nicholson, M. (2020, July 24). *Reshaping the cybersecurity landscape*. Deloitte Insights. Retrieved June 26, 2021, from https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html

Johnson, R. (2014). *Security Policies and Implementation Issues* (2nd ed., Kindle). Jones & Bartlett Learning.

Joint Task Force. (2012). *Guide for Conducting Risk Assessments* (SP 800-30, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Joint Task Force. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (SP 800-37, Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

MITRE. (2014). *Systems Engineering Guide*. The MITRE Corporation. https://www.mitre.org/publications/technical-papers/the-mitre-systems-engineering-guide

National Institute of Standards and Technology. (2004). *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199). U. S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.199

National Institute of Standards and Technology. (2016, November 30). *Overview*. NIST Risk Management Framework. Retrieved June 27, 2021, from https://csrc.nist.gov/projects/risk-management

National Institute of Standards and Technology. (2020). *Control Baselines for Information Systems and Organizations* (SP 800-53B). U. S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53B

PCI Security Standards Council. (2018). *Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures*. PCI Security Standards Council, LLC. https://www.pcisecuritystandards.org/document_library

Ponemon Institute. (2020). *Cost of Data Breach Report* (IBM Security, Ed.). IBM Corporation. https://www.ibm.com/security/data-breach

Ross, R., McEvilley, M., & Oren, J. (2016). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (SP 800-160, Vol. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v1

Schneier, B. (2008, September 2). *Security ROI: Fact or Fiction?* CSO. Retrieved June 27, 2021, from https://www.csoonline.com/article/2123096/security-roi--fact-or-fiction-.html

Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010). *Contingency Planning Guide for Federal Information Systems* (SP 800-34, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-34r1

Swanson, M., Hash, J., & Bowen, P. (2006). *Guide for Developing Security Plans for Federal Information Systems* (Special Publication 800-18, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-18r1

Touhill, G. J., & Touhill, C. J. (2014). *Cybersecurity for Executives: A Practical Guide*. Wiley.

Turpin, K., Pietrowski, W., Spencer, C., McGary, C., Causey, B., Petit, L., Scovetta, M. V., Manico, J., Coleman, J., Agarwal, A., & Petukhov, A. (2010). *OWASP Secure Coding Practices - Quick Reference Guide*. The OWASP Foundation. https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content