EasyChair Preprint

№ 8269

Information Security Architecture, Frameworks, and Implementation for T-Bay Company.

Aicha Abdi Moumin and Kuruvikulam Chandrasekaran Arun

June 13, 2022

Information Security Architecture, Frameworks, and Implementation for T-Bay company.

Aicha
Asia Pacific University
KL, Malaysia
aabdimounin@gmail.com

Dr. Kuruvikulam
Asia Pacific University
KL, Malaysia
kchandran.arun@staffemail.apu.edu.my

Abstract: information is gradually becoming one of an organization's most valuable assets. Every company needs information systems in order to access its data. Nevertheless, these systems must be trustworthy in terms of information confidentiality, integrity, and availability. Information security is a magical solution for these objectives, in which a system security audit is established to describe and prioritize the threats that threaten the information system's information assets. Information Security Architecture is extremely useful in directing security strategy at all levels. It gives you all the details you need to make the best decisions about which procedures and solutions to employ throughout your IT infrastructure, as well as how to manage the IT lifecycle. To be more explicit, the organization's Information Security Management System ISMS is concerned with securing information systems. An assessment and implementation of information security architectural frameworks at a global level have been produced in this article by defining, assessing, and implementing for the T-Bay firm, which is the study's aim.

The study again focuses on assessing and identifying T-present Bay's system flaws and risks, then recommending Information Security Architecture frameworks to improve T-IT Bay's security and protection while also allowing T-Bay to reform its system and become more broadly distributed. An ISO27001, COBIT, ITIL, and NIST have been built in this document to reduce and prevent the dangers that T-Bay corporate information systems confront. ISA frameworks give the necessary rules and procedures to help T-Bay minimize recognized risks and examine and improve its information security experience.

Keywords: ISO27001, COBIT, NIST, ITIL, Frameworks, Implementation, Suggestions/Recommendation.

Table of contents

Introduction

T-Bay is an international online shopping that works on planning and reservation services. The company is based in Kuala Lumpur, Malaysia. The enterprise's core competencies or service is the use of electronic transactions for its key customers and suppliers as part of the company's business strategy. It is regarded as one of the leading companies that provide IT services to travelers, with a primary goal of client happiness. Besides, we are concerned looking at the T-Bay's compliance with Information Security Architecture (ISA) which is basically a critical concept that is frequently targeted and required by businesses of all sizes. ISA is one of the greatest of the companies' priority lists, especially in this period, when breaking into people's personal information and erasing data becomes a job for some humans. Despite major technical improvements, information systems continue to fall short of addressing the ever-increasing expectations that businesses confront in terms of environmental protection and asset security. The main purpose of this approach is basically to ensure that IT security and business strategy are in sync. It facilitates the placement of security controls and countermeasures against breaches, as well as their relationship to the enterprise systems framework, it also raises awareness of potential dangers, difficulties, and risks to a company. A company's nervous system can be compared to the management information system. Its failure could have negative consequences across the board. Likewise, ISA is a tool for ensuring data confidentiality, availability, and integrity. An effective information security management system lowers the company's risk of a crisis. It also provides for the reduction of the effects of a crisis that occurs outside of the firm".

The aim of this research is to first analyze and demonstrate T-Bay company's current design concerns. Eventually, we'll figure out the issues/crises of the actual T-Bay systems. Then, we will try to propose some possible suggestions and assumptions. Simultaneously, the investigation will provide some of the top-rated frameworks that stand for IT security and protection. So, that could solve T-Bay's actual system crises and gave it a sort of re-engineering system.

I. T-Bay's current system issue assessment

With a strong yearly turnover of roughly $1.14 million, again, T-Bay International Online Shopping, situated in Kuala

Lumpur, Malaysia, is part of the travel planning and reservation services business. However, the company is presently aiming to reform its system for them to become widely spread. Despite the prestigious place that the company occupies it missing a full assessment on information security, its design is not perfect as it seems and has still not reached the implementation of the highest-rated international standard for IT maintenance, governance, and security. We were able to identify some of the enterprise likelihood weaknesses that can be an important risk to it, such as:

- Vulnerability: we found out that the company could be easily reached because it has inadequate physical security and also found that employees and visitors access the service almost the same way, things that cause damage to any organization.

- Lack of confidentiality within the company environment, otherwise between employees. Even though staffs work on different services and carry out different duties, stock, and archive different data some still leave their office laptops unlocked at all times, which can allow anyone to check/modify the data inside for any purpose.

- For the present design, sensitive standards such as PII (Personally identifiable information) have been defined to secure the data/information. Very simple to figure out who it is or what it is and easy to get into in an unauthorized way and hack.

- Data about nearly nothing: archiving non-essential records and storing various types of data can cause immense homogeneity and even the loss of interesting documents. In case alike may damage the company's reputation.

II. recommendation/assumptions for the previously identified risks

Besides, here are the possible solutions to which T-Bay can refer.

T-Bay must first apply some international industry standards with strong policies/controls and security architecture to expand into broader markets, however before doing so, here are some assumptions regarding the prior issues:

- Access security is a priority that cannot be neglected, especially in the business world, the question is all the more crucial. therefore, T-Bay must differentiate access and define a barrier by applying strong physical observative tools for its security.

-Applying high-security codes (long password, face recognition, or fingerprints) for the office laptops. In addition,

employees must be attentive and aware of the importance of what they are been responsible for. Therefore, the T-Bay manager should communicate and ascertain that all members of the organization have received proper training in order to perform their assigned information security-related roles and daily responsibilities.

- Stored data must be sorted and divided into categories to facilitate the services and put the company in a proper line. In addition, the value of the services they provide will grow, and there will be no loss.

III. Frameworks

Cybersecurity is critical for any company that manages a website or sells things over the internet. The majority of businesses now use cloud storage and have social media outlets online. T-Bay is a global company that specializes in online shopping. Its business model is mostly focused on electronic transactions. As a result, the necessity to protect its internet assets, such as data, and everything associated with it, would be vast and fascinating. Therefore, various IT security frameworks are available to assist enterprises in protecting themselves and reducing the exposure of organizations to vulnerability. Frameworks consist of a collection of documents that describe the organization's adopted rules, procedures, and processes. Therefore, it is critical for businesses to adopt an information security framework. As a result, the company will be able to gain the trust of the external world, particularly those who are connected to it. The methods outlined here will assist T-Bay in establishing the finest possible security system for her business. While each firm is unique, when it comes to developing a security strategy, they all ask themselves the same questions and are all about offering the best security and services. T-Bay company is traditional e-commerce that publishes information for customers so that it can adapt to any of them. Here are a few examples of Information security architecture frameworks widely used and essential for enterprises.

1. NIST Framework for cyber-security

Driven by industry and public demand in the United States, the NIST (National Institute of Standards and Technology) provides rules which can most of the time be applied to any organization and which therefore form a good working basis. It offers a company a set of rules, norms, and standards to help them strengthen its cybersecurity posture. Secretary of

Commerce Wilbur Ross stated, "Every company's first line of defense should be the voluntary NIST Cybersecurity Framework. For all CEOs, adopting it is a requirement." (News, 2018). NIST also works to better understand and management of privacy hazards, some of which are related to cybersecurity, and offer trustworthy networks. Foremost, the NIST framework has a three-tiered risk approach which are:

- Tier 1 is the organization and refers to the governance
- Tier 2 concern mission or business process and refer to the information and how it flows
- Tier 3 emphasizes the information system and includes the environment of operation

Besides, it has five core functions that contribute to the establishment of a solid business foundation and assist in the identification of cybersecurity compliance requirements and gaps. They are:

Identify: establish an awareness of cybersecurity risk to systems, assets, data, and capabilities within the company.

Protect: Aids in limiting a potential cybersecurity incident.

Detect: Enables the detection of cybersecurity movements on actual-time

Respond: Develop and implement suitable activities to respond to a cybersecurity event that has been detected.

Recover: establish and implement relevant steps to maintain resilience plans and restore any capabilities or services that have been harmed due to cybersecurity events.

2. ITIL Framework

ITIL (Information Technology Infrastructure Library) this framework was created in the eighth by the UK's government CCTA, to help organizations with their IT investments, responding to their business effectiveness and aims. (Techopedia, 2022). it is a widely accepted best practice framework for IT service management. ITIL includes practices, checklists, tasks, and procedures documenting the role of the ITSM function. This framework regards IT as a service emphasizing “Services”, so it helps the organization, plan and implements the best IT services for its customers. consists of five volumes/core publication. Each volume corresponds to a discipline, as follows:

Service Strategy: This volume serves to analyze the market and acknowledge all concerns, and a plan is designed to satisfy the demands.

Service design: This process is utilized to meet organizations and customers' requirements and it consists of eight other procedures

Service Transition: This's for deployment and administration of services.

service operation: This stage ensures that services are delivered on time.

Continuous improvement of services: Its mission is to enhance and develop services.

Therefore, the ITIL framework help organizations satisfy their clients.

3. COBIT framework

Certified as a well-known framework. This paradigm is used by all organizations whose business processes are related to technologies for reliable and relevant information. COBIT is also a framework for improving the sensitivity of IT processes used by both government and private sector organizations. The business orientation of COBIT involves tying a company's goals to its IT infrastructure by offering multiple maturity models and metrics for monitoring progress and defining business responsibility for IT activities. The fundamental focus of COBIT is illustrated by a process-based model organized into four distinct sections, which include:

Purchasing Organizing & Planning

Providing Support

Purchasing and Implementation

Observing and evaluating

This particular framework will be detailed and emphasized below.

4. ISO 27-001 framework

ISO 27001 is the only internationally recognized standard that establishes the requirements for an auditable information security management system (ISMS). ISO 27001's major purpose is to ensure the security of essential data assets in terms of confidentiality, integrity, and availability. The ISMS accreditation aims to benefit the organization by enhancing internal performance, ensuring customer confidence, assisting with compliance and regulation, managing internal and external security risks, and assisting with compliance and regulation. ISO 27001 accreditation makes sense for the firm when client, regulatory, or legal requirements need information security compliance. The following are the key advantages that any organization that implements this framework may reap:

- Creates a formal information security framework for putting security rules and goals in place.
- Ensures that customer, regulatory, and legal obligations are met.
- Enables the organization to give applicable security policies to prospective clients and pass security audits.
- Recognize and improve existing security procedures.
- Determine what level of business risk is acceptable for applicable security procedures.
- Lower the costs and dangers of security breaches, as well as ensure that the issue is handled effectively.
- Allows a third-party entity to independently certify the product.

IV.Security Frameworks for T-Bay company

The standards chosen for T-Bay are **COBIT** and **ISO-27001**. The reasons for choosing these two frameworks are multiple and we detail them below.

➢ Why COBIT?

Because the company aims to develop, monitor, and maintain its IT governance COBIT is the best framework. COBIT is meant for the governance and management of information and technology in the organization sector which might be an important ISA for T-Bay. It englobes the entire IT and data processing that firms use to meet their purpose because obviously, any enterprise with new standards design possesses an IT department that monitors every technology related. Furthermore, the research chose this particular framework for T-Bay because it is a framework for developing, implementing, monitoring, and improving IT governance and information management in businesses. T-Bay needs to protect its information assets with the greatest IT governance, management, and security standards. It wants to build, monitor, and sustain IT Governance, to be more explicit. COBIT has five principles functions:

- Responding to partners' requirements

-Taking care of the whole project

-Using a single and comprehensive framework

-Allowing for a more proactive strategy

-Separate governance and management.

Again, the research selected COBIT because it has the following benefit as well:

- keeping a balance between the use of available resources and the attainment of benefits while taking into account the hazards

- It also aids in the convergence of IT governance and enterprise governance, as well as all information and technology management procedures.
- allowing enterprises to have a single integrated framework that provides enterprise coverage and consistency, as well as the ability to modify it to their own needs

So, in a similar case, COBIT would be a fantastic choice for T-Bay to use and implement.

➢ How COBIT should be implemented:

COBIT Implementation comprises seven steps, which are:

Step 1: Identify the Needs of Stakeholders

The primary objective of every firm is to establish maximum operational resiliency in order to limit operational risks. This is achieved by implementing a sound business continuity plan that is backed up by the necessary rules and processes. This process may take a week for T-Bay.

Step 2: Determine the Enterprise and Alignment Goals.

T-Bay should be aware that the selection of enterprise goals (EG) and related alignment goals must be guided by stakeholder requests (AG). The goal is to ensure that business services are available and will remain so in the future.

Step 3: Identify the Governance and Management Objectives

This phase will necessitate for T-Bay to decide on appropriate governance and management goals. The key governance and management goals are as follows:

Evaluate the problem, direct it, and keep a careful check on it. Risk minimization is a given.

Make a plan for your safety precautions.

Construct, acquire, and put into action a Configuration that is modifiable

Three words come to mind when it comes to what we do: provide, serve, and support. The level of consistency was painstakingly maintained.

Third-party security services are known as managed security services.

Step 4: Choose and customize Enterprise and Alignment Goals and Metrics

The objectives and metrics can be changed and included as-is, or they can be utilized as key goal indicators (KGIs), key performance indicators (KPIs), or key risk indicators (KRIs)/areas, depending on T-Bay's reporting and monitoring system.

Step 5: Select and Customize the Governance and Management Component

COBIT offers quality practices and guidelines for each of the seven governance and management components, which T-Bay company can pick and choose from as appropriate.

Step 6: Create customized COBIT content and incorporate it into company procedures.

T-Bay can here so supplement the required COBIT content with guidance from relevant rules (where applicable) and other relevant suggestions. The information should then be translated and updated into specific rules, processes, standards, and guidelines that are included in various parts of the company's documentation.

Step 7: Confirm Results and Take Corrective Action Using Performance and Monitoring Measures

The necessary adjustments, as well as their benefits, should be communicated to the T-Bay governing body. To implement the new strategy as defined in the project plan and based on criticality, deliverables, and milestones, approval is necessary. Approval is also required for appropriate finance and change execution in the firm.

The whole process may take two (2) months to be accomplished.

- The second framework chosen for T-Bay is ISO-27001(incredibly intriguing).

➢ Why ISO-27001?

"Though there are more than a dozen standards in the ISO/IEC 27000 family, ISO/IEC 27001 is the most well-known, establishing specifications for an information security management system (ISMS). They allow any firm to manage the security of assets such as financial data, intellectual property, employee information, and information provided by third parties." (ISO.org). This framework is a security standard that service providers use to protect consumer information. The organization must be formally audited by an impartial and qualified authority to verify compliance. It contains a set of rules, processes, procedures, and systems for dealing with data violations and network hacking and it also responds to information security threats.

By implementing ISO T-Bay enterprise will receive many benefits like:

- The company will gain stakeholders' trust because Iso-27001 is an international certificate

framework and stand for information and data security.

- Data management standards that outline how certain data should be handled and shared are supplied by information security.
- Danger management: allows a corporation to limit who has the right to access certain information, reducing the risk of that information being stolen or otherwise compromised.
- Commercial Continuity: The process necessitates that the service is regularly tested and upgraded in order to assist the business operation.
- T-Bay will benefit an increased business resiliency as a result of this strategy.

Thus, the two frameworks will guarantee the company the improvements, development, security, integrity, and confidentiality within it and from outside environments.

➢ How ISO 27001 should be implemented:

Implementing ISO-27001 can be challenging but it is worth it as the proverb says "nothing worthwhile comes easily". ISO-27001 implementation requires nine (9) steps which are:

1. Assemble a team to implement ISO 27001

First and foremost, T-Bay must select a project manager in order to accomplish certain important goals as-is: the goal to be achieved, the time it will take, the cost the project will incur, and whether management agrees with it.

2. Create an ISO 27001 implementation strategy.

Then, T-Bay should have to be aware of the steps it is into and provide a detailed explanation of the purpose of the project but the risk that may arise in terms of security and the asset of the company after establishing high-level regulations of ISMS.

3. The initiation of the ISMS

Now it (T-Bay) must select a method of deploying the ISMS standard. Acknowledgment: the standard recognizes only one improvement continuity process approach and the most trusted paradigm for ensuring information security. However, this standard does not dictate to companies where they should limit themselves or continue with their model. So, the company must provide the rest of its documents.

4. Framework for management

The most important phase of this process for T-Bay is deciding on the scope of its

ISMS or what aspects of its business should have to be protected. It is crucial to define a clear scope ISMS implementation project.

5. Security controls at the very beginning

Here T-Bay company should create its security baseline using the information acquired during its ISO 27001 risk assessment.

6. Contingency (Risk) planning

This step is more about deciding how T-Bay will approach the job than avoiding hazards. This can be done in a variety of ways, but the majority of them involve looking at the risks to specific assets or hazards in specific situations.

Regardless of how it approaches the project, the risk assessment process is crucial.

7. Put the risk treatment plan into action.

Now is the time to implement a business-made/identified risk management approach. T-Bay should have to ensure that its employees can operate or engage with these controls and are aware of their information security duties to ensure they are effective. (And the employees of the organization have a key role to play in a cybersecurity strategy, which makes their training interesting. employees play a critical role in an organization's ability to operate in a safe and secure manner. It, therefore, becomes essential that employees have all the information and knowledge necessary to ensure the security of the network and information systems of an organization. Thus, they must be aware of the security risk related to their activities and how to cope with them, by respecting existing policies and procedures already set for the risks, attacks, threats, and so on.) T-Bay should also devise a strategy for assessing, reviewing, and maintaining the skills needed to achieve the ISMS objectives.

This requires conducting a needs analysis and identifying the desired skill level.

8. Assess, monitor, and evaluate

The review's main purpose is to see if T-Bay ISMS is genuinely preventing security issues, but it's a little more difficult than that.

Therefore, T-Bay should evaluate the project's results to the objectives that it specified previously in other words, what you planned to achieve.

9. Certification is number nine

Following the implementation of the ISMS, T-Bay should consider seeking certification from a suitable certifying authority.

This shows stakeholders that the ISMS is working and that the company cares about information security.

As part of the certification process, the organization's management system documentation will be reviewed to confirm that suitable controls have been implemented. The certifying organization will perform a site audit to put the procedures to the test.

Conclusion

Information is perhaps the most valuable asset in any modern corporation. The well-known CIA trinity of confidentiality, integrity, and availability is used to secure this information. Furthermore, information security is a risk management profession; the goal is to manage the risks associated with information leakage. The travel arrangement and reservation services industry include T-Bay International Online Shopping, located in Kuala Lumpur, Malaysia. to expand into new markets, it realized it needed major structural changes and reforms to improve its capabilities. As consultants, we offer the company this research by clearly explaining to it the methods and frameworks that it must implement and work on, the study also shows how it is implemented and what accompanies it. So that it widens the frontier and improves its services and missions.

References:

- Abdul Rafeq& Narasimhan Elangovan. (26 May 2021). INDUSTRY NEWS: A Systematic Approach to Implementing a Governance System Using COBIT 2019.ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2021/a-systematic-approach-to-implementing-a-governance-system-using-cobit-2019

- Al-Daeef M.M& Basir N& Saudi M.M. (2017). Security awareness training: A review. Newswood Limited. https://oarep.usim.edu.my/jspui/handle/123456789/1880

- Ethan Bresnahan. (n.d). CyberSaint Security. NIST Cybersecurity Framework Core. https://www.cybersaint.io/blog/nist-cybersecurity-framework-core-explained#:~:text=Here%2C%20we'll%20be%20diving,common%20across%20critical%20infrastructure%20sectors.

- ISACA Now. (30 Jun 2021). 3 things COBIT is and 3 things it isn't.https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-19/3-things-cobit-is-3-things-it-isnt

- ISO/IEC 27001. (n.d). Imperva. https://www.imperva.com/learn/data-security/iso-27001/

- Jan Killmeyer. (13 Jan 2006). Information Security Architecture: An Integrated Approach to Security in the Organization, 2nd Ed. NewYork.https://www.taylorfrancis.com/books/mono/10.1201/9780203488751/information-security-architecture-jan-killmeyer

- Wawak, Slawomir (2010): The Importance of Information Security Management in Crisis Prevention in the Company. Published in: Global Economic Crisis and Changes (2010): pp. 638-645. https://mpra.ub.uni-muenchen.de/47959/