Mutiara bank case study

Business

So far, it has a good security system. When we came inside the building, the security guard told us to do the security checking first, and next they asked us what do we want to do and which floor are we going to, and then we are required to leave our IDs and exchanged it with a security pass so that we can come inside the office. When we arrived in our designated floor we went to the receptionist, and she told us to wait. When were waiting, we tried to observe the surrounding area.

To enter the office an ID is required to pass, and all the guests need to wait outside the office area.

Here we can conclude that the security that they implement is good. In which, they are limiting the access to their office area. After a long time of waiting, we finally meet with the person in charge. We asked few questions regarding our company visit, however we were not able to conduct the Interview relent away.

I nee person salad Nat It was tenet Dustless week Ana nee couldn’t guarantee that the person who can answer our questions agreed on doing the interview. So instead, we were asked to send the questions through email.

After several days, we finally got the questions filled, and will be explained on the next section. 4. 3 Minutia Bank Audit of Information Systems Following the Bank Indonesia Regulation / “ Perpetual Bank Indonesia” (BPI) No.

9/1 5 Than 2007, about the Electronic Banking which stated that “ any plan to publish Electronic Banking products which are transactional in nature must be included in he Banks Business Plan and submitted to Bank Indonesia 2 (two) months before said product(s) are published.

The report must be complemented with, amongst others, results of analysis conducted by independent parties on the characteristics of the product and sufficiency of Information Technology security. Banks must educate customers on its Electronic Banking products and its security. ” Q Technologies has been appointed by OPT. Bank Minutia Tab.

(Bank Minutia) to implement Security Assessment for Electronic Banking in order to comply with “ Perpetual Bank Indonesia” (BPI) to find out whether if there is a gap for security reach in both applications and infrastructure for electronic banking.

The technical overview of this security assessment for application and infrastructure project is describes as follow: Testing service proactively attempts to break into the system to assess Bank Minutia’s level of security preparedness. This activities help Bank Minutia to get a hacker’s point of view of the system, and It enables Bank Minutia to identify security holes that could be exploited by a remote attacker to compromise the system.

The software brought many advantages to Minutia Bank such as: Categorization of nakedness based on risk level Details of security holes discovered Emergency quick-fix solution for discovered vulnerabilities Use your application with the confidence that it is secure Eliminate threats by raising the threshold for potential intrusions Theft and fraud Give

stakeholders in your application tools that meet the highest security standards and; Reduce customers' security concerns. 4. 4 Minutia Bank Information Security Systems Minutia bank definitely faces IT challenges related with information system being used, as for current system.

Minutia bank has achieved speed and flexibility required or product development. Thus, the likely for security breach to happen increases, Ana In order to protect ten system Mutual Dank uses unaware security module to protect its systems from any breaching. When asked about whether there has occurred a hacking or loss of data, up until now, there has never been any hacking or data loss occurring. They really emphasize in protecting their security systems, so that they can operate smoothly to satisfy their customers. Whereas, in order to prevent hacking or data loss they are using hardware form several vendors.

One of he vendors known is Q Technologies, which is appointed by Minutia Bank implement Security Assessment for Electronic Banking The use of Minutia Bank in business (specifically IT development) isSupremein terms of the system's infrastructure to assure the safety and the satisfaction of delivering the product. Minutia has specific program to assure employees information are being recorded accordingly. Data access in Minutia Bank is also limited to certain department. Only those that have the authorization can access customers' database. It means that Minutia bank emphasizes the application of a good segregation of duties.

In Indonesia lots of natural disaster are happening quite often, which includes flood, earthquake, and fire. In order to satisfy customers and

continuing the operations when a disaster happens, Minutia Bank has a disaster recovery plan to overcome this. However, the exact plan cannot be revealed due to the policy of the company. In order to continue the operating activities, many companies are insuring its information systems. The same goes with Minutia bank, which is in order to ensure that the operating activities can be performed without any interruptions from the mage in the system; Minutia bank has its information systems insured.

Security control plays a vital role in an organization, whereas it helps the company to prevent hacking from outside.

There are three types of security control which are; Preventive, Detective, and Corrective control. For Minutia bank, security control is very important, and they do have the preventive, detective and corrective control. However, it cannot be disclosed further due to the policy of the company. 4. 5 Theory Analyses In the theory analysis, CUBIT 5 Framework will be used as guidance to asses Minutia Bank Accounting Information Systems.

CUBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. It includes all aspects of ensuring reasonable and appropriate security for information resources. Its foundation is a set of principles upon which an organization should build and test security policies, standards, guidelines, processes, and controls: 1. Principle 1 : Meeting Stakeholders’ Needs A group of stakeholders includes any individual or group affected by the current state or future state of a process, system, policy, etc.

Stakeholder analysis is the process of identifying stakeholders so that their input can ensure outcomes match requirements. This is an important step in both project planning and risk management.

Failure to involve all stakeholders, including Infuses and audit teams, usually results in less than optimum outcomes at best. Worst-case outcomes include failed projects or material audit deficiencies. In carrying on its operations, Minutia Bank is seen to have satisfied the stakeholders, and that the input can be matched against its output.

In order to do so, Minutia Bank together with Q Technologies eave implement Security Assessment for Electronic Banking in order to comply with Dreads In Don applications Ana Understructure Tort electronic Dankly. 2 Principle 2 Covering the enterprise end-to-end Information security is often applied as series of point solutions, as defined in more detail in Principle 3.

However, general application of security and assurance best practices requires security reviews as part of all business processes and IT development and implementation activities. This isn’t Just a horizontal integration.

For example, a department vice president might implement a new business process thou consulting audit or security. If the organization has a solid security program, the UP is aware of and supports it, and C-level executives are clear in their requirement that each business process must conform to the program, then the new process will likely meet expected security outcomes: even without security and audit reviews. However, engaging

Infuses and audit teams to review major process changes is always a good idea: regardless of how “ safe” or “ insignificant” the change appears.

In Minutia Bank, we cannot defined whether they have a solid security systems. This is due to the lack of information provided, however, from the information obtained it’s said that Minutia Bank uses hardware from various vendor to prevent any hacking or data losses. This can be interpreted that they have quite a good security systems, besides that they have audit committee in their organizational structure which helps to ensure that the security systems is implemented correctly. 3. Principle 3 : Applying a single integrated framework Application of security controls is often a point-and-shoot activity.

Many organizations tend to fix specific issues without stepping back and applying policies ND controls that impact multiple vulnerabilities in network or system attack surfaces. Designing a complete framework includes all aspects of information storage, flow, and processing, providing a foundation for more efficient control implementation. One method of ensuring optimum use of controls is creation and management of a controls matrix, as shown above. It is really important to have a good security control. In Minutia bank, they do realize the importance of this and applying it too.

They have preventive, detective and corrective control to guard their security systems.

However, not much information can be obtained regarding this matter. However, we can conclude that Minutia bank has comply to this principle. 4. Principle 4 : Enabling a holistic approach As support for developing an

integrated framework, it’s important to see information security as a set of related components: not as set of silos. Each component is driven by enablers and other factors affecting organization risk. CUBIT 5 for Information Security provides a list of enablers and describes how they interrelate as shown in Figure below.

Enablers help organizations integrate operations and security into the outcomes of all principles defined here. As always, this is done in a way to meet stakeholder requirements. For Mutual Bank, ten same applies as Delve, several endless are explain as : Boo IT and business teams use processes to get work done with consistent outcomes. Security teams must include how work is done when designing a security framework and program. An organizational structure (a management hierarchy) is designed to monitor and reach strategic and operational objectives.

Leaders (decision makers) from each level are typically stakeholders in business processes and expected outcomes. An organization is a living entity, with its own culture, ethics, and behavior as exhibited by its employees. Changing the way employees see their working world is not easy and must be considered when trying to secure the workplace. Information is what we attempt to protect…

And it is usually everywhere. In most cases, information is critical for business operations and must be available when and where needed. Further, access to the data should not come with unacceptable response times caused by poorly designed security controls.

IT delivers information via services, infrastructure, and applications. All security control implementations require attention to people, skills, and competencies: both in and out of IT.

For example, is it more appropriate to enforce a policy with technical controls, or are the employees able administratively to meet expected risk outcomes? Principles, policies, and frameworks provide the means to integrate all enablers into an overall solution resulting in secure operational success. The enablers help achieve the outcomes expected when developing principles, policies, and frameworks.

It can be said that Minutia bank has a good holistic approach, and has implied with this principle. 5. Principle 5 : Separating governance from management This principle establishes a line between setting objectives and measuring outcomes. According to CUBIT 5 for Information Security, Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balances, agreed-on enterprise objectives to be achieved; setting direction through pronunciation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

It is important to separate the governance and management of a company. Therefore, this should also be implemented in Minutia Bank, in order to endure that stakeholders' needs are being met to fulfill the objectives. There has no indication about separate governance and management. However, it can be seen that Minutia bank has tried to fulfill stakeholders' necessities in order to satisfy them. CHAPTER 5 5.

1 Conclusions From all ten above assertions, Interviewing Ana analyses, It can eve seen Tanat Minutia Bank has a really good security systems.

Whereas, the information systems implemented is really good that there has never been any hacking or data loss up till current operations. Just like what has been mentioned earlier, Minutia Bank pointed Q Technologies in order to implement to implement Security Assessment for Electronic Banking in order to comply with " Perpetual Bank Indonesia" (BPI) to find out whether if there is a gap for security breach in both applications and infrastructure for electronic banking.

This means that, the security systems are expected to be high, so that it complies with the government regulations, and therefore the stakeholders demands can be met. Since minutia bank highly engaged in the information technology, it is really important to have a good security plan, like natural disaster recovery plan whereas it as accomplished to ensure that when a disaster occur, they can start to operate immediately.

Besides, that no hacking or data losses have occurred, this means they really have implemented a good information security systems.

Not only date authorization plays a vital role in their daily operations, they also limit the data access, which is really good. This means segregation of duties and security are highly emphasized. Overall, Minutia Bank has a really good information systems and very tough firewalls and security systems, because no data loss and hacking have ever occurred, up till these days.