Analysis of Data Center Risk Management in Indonesia National Traffic Police Corps

Wita Susilowaty

Abstract

Topic about Data Center crisis highlighted that significant risk failures persist despite the investments in the disciplines of risk assessment and risk management. Although isolated incidents of one-time governance failure are reduced, the systemic ruin are more than just a stray differentiation. Various experts and professional institutions dealing with risk management have come to the judgement that the failures may be caused by a confusion in the risk information due to diverse risk assessments from different point of view [3][6]. The Data Center crisis and the resulting regulatory pressure forced the chief data center officers and high ranked management of Indonesia Traffic Police Corps to focus more on assessment, mitigation and reporting of risk. The process of organizing these risk assessments to provide the Indonesia Traffic Police Corps with a more holistic view of the enterprise risk is fundamental to mastering risk assessment.

Keywords: Data Center; Risk Management.

Introduction

Indonesia National Traffic Police Corps is one of the institutions in charge of traffic and road transport. To support the tasks and responsibilities, they built traffic and road application and systems that is placed in the Data Center, called NTMC Data Center. The NTMC Data Center has almost close to the standard Tier 3.

The terms availability, reliability, mean time between failure (MTBF), and the others are often used interchangeably to describe data center performance [1]. However, the management of NTMC Data Center not currently applied risk management and failure, so vulnerable a system failure occurred due to the absence of prevention.

Risk assessment is a part of the overall discipline of risk management. Risk is defined as the suspicion of an event appear that could have an effect on the achievement of objectives. The definition of risk assessment then follows as the identification, estimation and evaluation of the levels of risks involved in a situation, their comparison with benchmarks or standards, and determination of an acceptable level of risk. Risk assessment should answer the following questions: what can go wrong, how can it go wrong, what is the potential harm, and what can be done about it.

1. Data Center Risk Management

1.1. Challenges in the Datacenter

Every institutions face the challenges about how to manage datacenter, like delivery of reliable services, operational efficiency, and improved business responsiveness [8].

a. Delivery of Reliable Services.

Data center must provide high available services and full uptime in a reliable and predictable situation. IT manager must have a holistic and operational view with their datacenter environments [8].
b. Improved Business Responsiveness.

There is a high expectation on IT to be agile and responsive with business needs. Because of that, institutions have started to investigate cloud solutions. Nonetheless, many are unsure about how and where to begin making a transition [8].

1.2. Risk Identification

The basic step of risk management is risk identification. This step determines the highly occurring potential risks, and other events which occur very frequently [7]. Risk is investigated by looking at the institutions activity in all directions and attempting to introduce the new exposure which will arise in the future from changing the internal and external environment. Correct risk identification guarantees risk management effectiveness [9], and will helps the management to identify the forthcoming risk from any direction at the initial stages in order to avoid overlapping of the process in the future outcomes.

1.3. Risk Evaluation

Risk evaluation is very important in specific situations and provides adequate material for make decisions [11]. This step will show whether risks are acceptable or need treatment. Evaluation means whether to accept the risk or not. If it is accepted, the management should decide at which position they could handle the situation, and if they cannot handle, what is the further process to be undertaken. Thus evaluation plays a vital role in the risk management to consider the tolerance of risk, which depends on the voluntary association.

1.4. Risk-based approaches

Many groups within an institution risk assessment are increasingly conducted by to fulfil a variety of business and regulatory requirements. Various groups in the same institutions often depend on guidance from different professional institutions to provide a framework for directing the risk assessment. As these professional institutions offer disparate approaches to risk assessment, they contribute to a huge of risk information. In this context, information systems and/or information technology (IS/IT) of risk assessment take parts in an entirely exceptional role in each institution. There are two reasons for that statement [10]. The first: IS/IT integrates all different functional domain within an institution and it has a prospect to combine the risk assessment activities as well; the second: IS/IT deals with data or information processing and by organizing it risk will reduce unvaluable information. In the same time, we enhance the quality of business processes, as information is the important pieces of each business process. According on the hypothesis, we can conclude that there is no use to create a dissimilarity between business risk and IS/IT risk. IT risk is specifically business risk, the business risk related with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise [4].

The business value and Information Technology risk are two sides and risk is inherent to all enterprises. At the same time, to eliminate all the risks, we can jeopardize the profit driving opportunities. In practice, there is no single unified solution to the complex situation mentioned. Therefore, there are many various risk assessment frameworks aiming at different purpose and different tools.

1.5. The Risk IT

The scope of the Risk IT framework is also covered with the scope of the COBIT 5 framework [4]. To implement Risk IT framework, we need to review the COBIT 5 framework first, if it need more guidance on risk, reference the Risk IT publications for more detail. While COBIT provides a set of controls to mitigate IT risk, Risk IT present a framework as a tool to identify, govern and manage IT risk. Simply put, COBIT presents the means of risk management; Risk IT provides the ends. Enterprises who have use (or are planning to use) COBIT as their IT governance framework can adopt Risk IT to enhance risk management.

2. Methodology

Before integrate existing framework in analysis, first thing to do is understand how the frameworks work individually and then conduct a detailed study about how the frameworks can be integrated. The methodology used consists of the following steps:
a. Review and study of existing literature.
b. Analysis data using COBIT frameworks.
c. Mitigation of gaps based on previous study and research and current analysis result.

The purpose of this analysis is to get clear traceability with integrated framework using a top down approach. To achieve this, it is critical to ensure that the output of one framework is aligned perfectly with the input of the other framework, thereby establishing a robust input-process-output methodology.

3. Data Analysis

In order to do an assessment of IT Risk Management in NTMC Data Center, COBIT framework is used to determine the risk level of the data center.

3.1. Process AI3: Acquire and Maintain Technology Infrastructure

3.1.1. Control Objective AI3.1 – Technological Infrastructure Acquisition Plan

Prepare and produce a plan or strategy for the acquisition, implementation and maintenance of the technology infrastructure that can established functional of business and technical requirements and is in accord with the institution’s technology policy.

Conclusion: Objective Not Met

Observations: The NTMC Data Center has compiled a formal set of information technology standards. However, this document did not include standards for the technological infrastructure.

Risks: If the Indonesia Traffic Police Corps does not establish technological infrastructure standards, then the impact:

1) May acquire and install hardware and/or software that are not compatible with the Indonesia Traffic Police Corps technology and Infrastructure.
2) May acquire and install hardware and/or software that are not consistent with the Indonesia Traffic Police intended technology direction.

3.1.2. Control Objective AI3.2 – Infrastructure Resource Protection and Availability

With the implementation of internal control, security and auditability, and then measures them during configuration, integration and maintenance of device or hardware and infrastructural software to guard resources and assure availability and integrity. Responsibilities for implement sensitive and crucial infrastructure components should be defined very clear and can be understood by developer and integrator infrastructure components. Usage of infrastructure components should be monitored and evaluated.

Conclusion: Objective Not Met

Observations: The Indonesia Traffic Police Corps’ IT control environment has a lacks critical policy, procedure and guideline documentation.

The Indonesia Traffic Police Corps relies heavily on the knowledge and dedication of an experienced IT staff. The Indonesia Traffic Police Corps division does control changes to the infrastructure by change management process. However, the Information Technology Departement of The Indonesia Traffic Police Corps does not have policies, procedures or guidelines that documented for capacity management and monitoring.

Risks: Capacity Management / monitoring practices may not be effective in determining the need to increase bandwidth, address root-causes, or report on usage presenting potential risks to network and system availability.

3.1.3. Control Objective AI3.3 – Infrastructure Maintenance

Prepare and build a strategy and plan for infrastructure maintenance, and ensure that changes are according to the institution’s change management procedure. The procedure might include periodic reviews against institution needs, patch management, and upgrade strategies, risks, susceptibility assessment and security requirements.

Conclusion: Objective Met

Observations: Based upon work performed, it feels this objective is being satisfactorily met due to infrastructure changes being subject to the Indonesia Traffic Police Corps’ IT Change Management Process Policy. The policy requires review of change requests by the Change Advisory Board, which consists of the Indonesia Traffic Police Corps IT Department's Senior Management team. The Change Advisory Board meets on a weekly basis.
3.1.4. **Control Objective AI3.4– Feasibility Test Environment**

Establish development and examine the environments to support effective and efficient practicability and integration testing of infrastructure components.

**Conclusion:** Objective Not Met

**Observations:** The Indonesia Traffic Police Corps does not have development and examine the environments to support effective and efficient practicability and integration testing of infrastructure components.

**Risks:** Changes to the production environment may present security, integrity and availability risks to the computing environment.

3.2. **Process DS12: Manage the Physical Environment**

3.2.1. **Control Objective DS12.1– Site Selection and Layout**

Define and select the physical location for IT devices to support the technology strategy linked to the business strategy. The selection and layout of a location should take into account the risk associated with natural and man-made disasters. Beside that, it should considering relevant laws and regulations, such as regulations of occupational health and safety.

**Conclusion:** Objective Met

**Observation:** Based upon work performed, it feels this objective is being satisfactorily met due to the location and layout of the Indonesia Traffic Police Corps data center appears to support the business needs of the Indonesia Traffic Police Corps and appears to take into account risks associated with natural and man-made disasters.

3.2.2. **Control Objective DS12.2– Physical Security Measures**

The definition and implementation of physical security scope with business needed to secure the site and assets. Result of measures physical security must be effective and capable of preventing, detecting and mitigating risks relating to theft, temperature, air flow, fire, smoke, vibration, water, humidity, terror, power outages, chemicals, disasters or explosives.

**Conclusion:** Objective Met

**Observations:** Based upon work performed, it feels this objective is being satisfactorily met due to the following physical security controls being in place at the Indonesia Traffic Police Corps Data Center:

1) Data center housed in a secure facility
2) Camera with video feed for remote viewing
3) Card key required to access Data center
4) Alarm system for the data center
5) Server enclosures restrict access to authorized IT personnel.

3.2.3. **Control Objective DS12.3– Physical Access**

Define, describe and implement procedures to grant, limit and revoke access to sites, buildings and location based on business needs, including emergencies. Access to sites, buildings and areas should be justified, authorized, logged and supervised. This should apply to all those who entered the site, including staff, members, temporary staff, employees, clients, vendors, contractors, visitors or any other third party.

**Conclusion:** Objective Met

**Observations:** Based upon work performed, it feels this objective is being satisfactorily met due to data center personnel access the data center via card key and all other Indonesia Traffic Police Corps employees, contractors, vendors, visitors and other third parties are required to sign in prior to entering the data center.

3.2.4. **Control Objective DS12.4– Protection against Environmental Factors**

Design, define and implement measures for protection against environmental factors. Also install specialized equipment and devices to monitor and control the environment.

**Conclusion:** Objective Met

**Observations:** Based upon work performed, it feels this objective is being satisfactorily met due to the following Environmental Controls existing at the NTMC data center:

1) Fire / Heat / Smoke / Humidity Monitoring
2) Dry pipe sprinklers.
3) Raised Floor
3.2.5. Control Objective DS12.5—Physical Facilities Management

Manage and control facilities, including power, network, communications equipment, in line with laws and regulations, technical and organization or business requirements, vendor specifications, and health and safety regulations / guidelines.

Conclusion: Objective Met

Observations: Based upon work performed, it feels this objective is being satisfactorily met due to the following physical facility controls existing at the NTMC Data Center: UPS Battery (60 min capacity) and Backup Generator, Two separate electrical feeds from power company (AEP), Raised Floor.

4. Future works

This research present a comprehensive framework and subject to any number of limitations in analyzing by just using COBIT 5 framework. In future work, the limitations of this research might be explored and combine with other framework like IT Risk in analysis to get more comprehensive analysis and results.

5. Conclusion

This research presents a comprehensive framework and analyze the NTMC Data Center Risk using COBIT 5 framework. Result of the analyze are that The NTMC Data Center doesn’t establish technological infrastructure standards and may affect incompatible technology and infrastructure that acquire and install and inconsistent hardware and software that acquire and install in data center; the IT department does not documented policies, procedures or guidelines for capacity management and monitoring. Capacity Management / monitoring practices may not be effective in determining the need to increase bandwidth, address root-causes, or report on usage presenting potential risks to network and system availability; and they don’t have development and test environments to support effective, efficient, and competent feasibility and integration testing of infrastructure components, it may present security, integrity and availability risks to the computing environment.

According to the analyze result, to reduce the risk in NTMC Data Center needs to take the following steps:

a. Indonesia Traffic Police Corps must prepare and establish a formal set of information standards. With this standards, will reduce incompatible hardware and/or software that implement in NTMC Data Center.

b. Indonesia Traffic Police Corps must formulate critical policy, procedure and guideline documentation to control, security and auditability implementation hardware, software, and infrastructure in data center.

c. Indonesia Traffic Police Corps should have development and test environment that different with production environment. This will support effective, efficient, and competent feasibility and integration testing of infrastructure components.

References