INTERNSHIP REPORT

Submitted To

Mr. Shamim Ahmed

Lecturer

BRAC Business School

BRAC University

Submitted By

Ajmain Fayek Afnan

ID: 14104079

Date of Submission

December 18, 2018

Taskeater

“Data Classification and Information Security Management System (ISMS) Awareness”
At
Taskeater Bangladesh Limited

Letter of Transmittal

18th December 2018

Mr. Shamim Ahmed

Lecturer

BRAC Business School

BRAC University 66, Mohakhali, Dhaka 1212.

Subject: Submission of internship report on "Data Classification and Information Security Management System (ISMS) Awareness" at Taskeater Bangladesh Limited.

Sir,

With due respect, this is to inform you that I have successfully completed my internship report and I would like to convey my sheer gratitude towards you for the immense support you have given me regarding the preparation of this report, throughout the whole term. It would never be so easy for me if I had not got the full support from you. Since I was a full time employee at Taskeater Bangladesh Limited I have explored the company's ins and outs, which I would not be able to do if I was an intern. I have been working as an analyst, on two departments, which are 1. Data Processing and 2. Lead Generation, under the supervision of Ms. Imratul Jannat- Manager, Operations.

This report contains a brief introduction to data classification and information security management system (ISMS) and how the organization is maintaining it, also the efficiency and effectiveness of maintaining these are included too.

I have attempted my level best to abide by the instructions that you had given me and I wish this report will meet the standard of your judgement. Thank you.

Sincerely,

Ajmain Fayek Afnan

ID: 14104079

BRAC Business School

BRAC University

Letter of Endorsement

That is to certify that Ajmain Fayek Afnan is a student of BRAC Business School, ID: 14104079, Major in Accounting and Minor in Finance, has successfully completed his "Internship program" entitled "Data Classification and Information Security Management System (ISMS) Awareness" at Taskeater Bangladesh Limited under my observation as the partial fulfillment for the award of BBA degree.

He has executed everything according to my instructions and has tried his best to do that resourcefully. I suppose this program will succor him within the destiny to assemble his career. I want his attainment and glowing fortune.

Signature

……..……

Mr. Shamim Ahmed

Lecturer

BRAC Business School

BRAC University 66, Mohakhali, Dhaka-1212, Bangladesh

Acknowledgement

The successful completion of this internship report is the result of the contribution and association of a number of persons, particularly those who took the time to share their thoughtful path and suggestions to develop the report. I have the deepest feeling to my revered supervisor and mentor Ms. Imtratul Jannat, Manager- Operations at Taskeater Bangladesh Limited. I am glad to her for her continuous support, guidance and direction, recommendations and providing me with valuable data that was meaningfully required for the accomplishment of this report. I am furthermore grateful to Mr. Abdullah Ibne Latif- Manager, Data Security and Compliances for giving me information related to my report, Mr. Asif Iqbal- Finance Manager, for giving me the idea of the financial benefits of adopting the awareness and supporting me with data and resources. I am also grateful to the HR executives, who have given me information that I was badly in need within a short period of time. I am additionally grateful to the complete Taskeater family as they have been there whenever I had required them. Their active participation to all my questions, queries during my office has created this journey a real accomplishment. It absolutely was my privilege and a good opportunity and I am honestly grateful working with such a beautiful team. Finally my sincere feelings go to my family, friends, classmates and colleagues who helped me whenever I was in need.

Executive Summary

This paper is about the study that I have gone through during my running employment in Taskeater Bangladesh Limited as an Analyst in the departments; Data Processing and Lead Generation. The study is about Data Classification and Information Security Management System awareness which falls under the subject Management Information System. Though being an accounting major, I have done my study based on MIS because I have interest in the IT industry. This paper firstly provides an introduction to the topic and to the organization that I am currently working in right now. After that, I have briefly discussed about how my organization has adopted the ISMS awareness and Data Classification processes to maintain the security of its own information and its client's information as well. The effectiveness and efficiency of the study has been discussed in the later part of the paper. According to my own understanding, this paper does not have the information fully since my company is strict regarding the confidentiality of information. However, as a full time employee, I got the privilege to collect maximum of the information and used them in my study.

Contents

Chapter 01: Introduction

1.1 Business Process Outsourcing

Firstly, to understand the whole paper, a brief introduction of Business Process Outsourcing is needed. Business process outsourcing (BPO) is a technique for authorizing different business-related tasks to outsider merchants. At the point when business process outsourcing started, it connected mainly to manufacturing substances, for example, soda pop producers that redistributed substantial fragments of their supply chains. Nonetheless, various services have been outsourced in the present world.

Associations take part in business process outsourcing for two primary regions of work: back-office functions and front-office functions.

Associations can outsource a range of back-office functions (additionally indicated to as interior business functions) including bookkeeping, IT administrations, Human resources, quality assurance (QA) and payment proceedings.

Likewise, Front office functions can be outsourced as well, for example, Customer Relationship Management (CRM), advertising, and sales.

Organizations can equally outsource specific functions like payroll, in those areas aside outsourcing a whole functional area (i.e., HR).

Business Process Outsourcing was first introduced in Bangladesh in 2008 and till now there are about 100 companies where almost 40,000 youngsters are working. According to Hossain, a local and leading entrepreneur in the sector, the number of youngsters working in the outsourcing sector are likely to be reaching 100,000 by 2021.

Towhid Hossain, secretary general of the Bangladesh Association of Call Centre and Outsourcing (BACCO) says “Companies in the sector now hope to hit the $1-billion mark soon’.

So, basically, Bangladesh has been trying hard to be a

worthy competitor in the global outsourcing market but unfortunately the Bangladeshi companies are hardly grabbing $180 Million of the $500 Billion of global outsourcing market.

1.2 Data Classification and Information Security Management System

Data classification has become a big deal for any company that reserves confidential data. Classifying the data in different criteria can be helpful for any company in terms of maintenance. On the other hand, the introduction of Information Security Management System has been a blessing towards the organizations that contain confidential information and also to the organizations that outsource their valuable information. Information security management basically describes the process that an organization needs to apply to make sure that it is reasonably guarding the privacy, availability, and integrity of possessions from threats and vulnerabilities. Taskeater has successfully been protecting the information that it contains within the premises of its operations and also the servers that it operates within.

1.3 Objectives of the Study

The objectives behind this study are:

1. Principal Objective:

   To discuss the effective methods that Taskeater Bangladesh Limited has been adopting overtime to secure its information and classifying the data within , also the effectiveness and efficiency of the Information Security Management Systems Awareness within the company, and also the benefits that the company has been adoring in this regard.

2. Secondary objective:

   The report is a prerequisite for the completion of BBA degree from BRAC University.

1.4 Scope of the Study

This report will be covering Data Classification and Information Security Management System Awareness at Taskeater Bangladesh Limited. The study is based on research, knowledge acquired from Management Information System (MIS) and experience of working as an analyst in the organization.

1.5 Methodology

The entire project was completed in a precise way, from selecting the topic till the completion. The main step was to choose the topic, about which I had discussed with my internship supervisor, Mr. Shamim Ahmed. Under his proper supervision and support, I sensibly chose this subject to work on. Secondly, data sources, both principal and subordinate were required to be acknowledged, measured and considered in order to perform this study. Finally, a big share of all the material presented here are collected from working in the office practically and discussing with the current personnel of the company and also with my supervisor at office as well as from Akkroo, 9Fin, Mixcloud (clients), within my employment period at Taskeater, so far.

To complete this study, primary data were gathered from my line manager, finance manager and IT Manager and also by talking to my clients and my colleagues. Moreover, direct observation of my supervisor and the experience I have gathered within the duration of my employment so far have also helped me to learn and present relevant material to the topic in discussion of this project. On the other hand, some of the secondary data were obtained from the website of the organization. Besides, I have consulted a few previous researches and also a few journals in this regard. Every relevant information sources are mentioned at the end of this report, in the reference part.

1.6 Limitations of the Study

- The topic being relatively new, it was hard for me to find out enough relatable research papers or journals which could have completely enlighten me to frame my paper.
- Lack of appropriate articles, publications and documents related to my topic was also a problem during the research.
- The time is another lacking of the report. If I had got a few months more, then I could have gone more deep into the exploration and find more valuable facts.
- Lastly, Taskeater Bangladesh Limited is very strict about the privacy of the information contained within the premises as well as the server. So, as a full time analyst in the organization, I extracted as much as I could get but I feel that those were not adequate to perfectly complete my research.

Chapter 02: Company Overview

Taskeater Bangladesh Limited builds extended teams for internet companies operating primarily in Europe. Taskeater's teams support clients in areas such as data processing, back-end operations, content moderation, lead generation, and online marketing. It sets up ongoing dedicated teams that work directly with clients. Clients view this company as a way to outsource certain processes so that they can focus on innovation and the areas that are core to their competitive advantage.

The company's current and past clients are from around the world, including from Finland, Sweden, Denmark, Holland, United Kingdom, Australia, United States, Lithuania, France, Canada and Germany.

2.1 History

- Founded in March 2014 as a Finland-based organization with its core office in Dhaka, Bangladesh.
- In March 2015, Taskeater Bangladesh Limited was integrated to support the growing organization in Dhaka.
- In August 2015, Taskeater hired its first Europe-based employee in London to beginning building its international sales Organization.
- In February 2017, Taskeater moved into its first commercial office premises in Mirpur.
- As of July 2017, it had 220 employees and as of September 2017, it had 280 employees.

2.2 Company Goals

Rather than having mission or vision statements, this company has two clear goals:

1. To become a brand of choice for high growth corporations in Europe for outsourcing.
2. To become an employer of choice for young professionals in Bangladesh.

2.3 Company Culture and Values

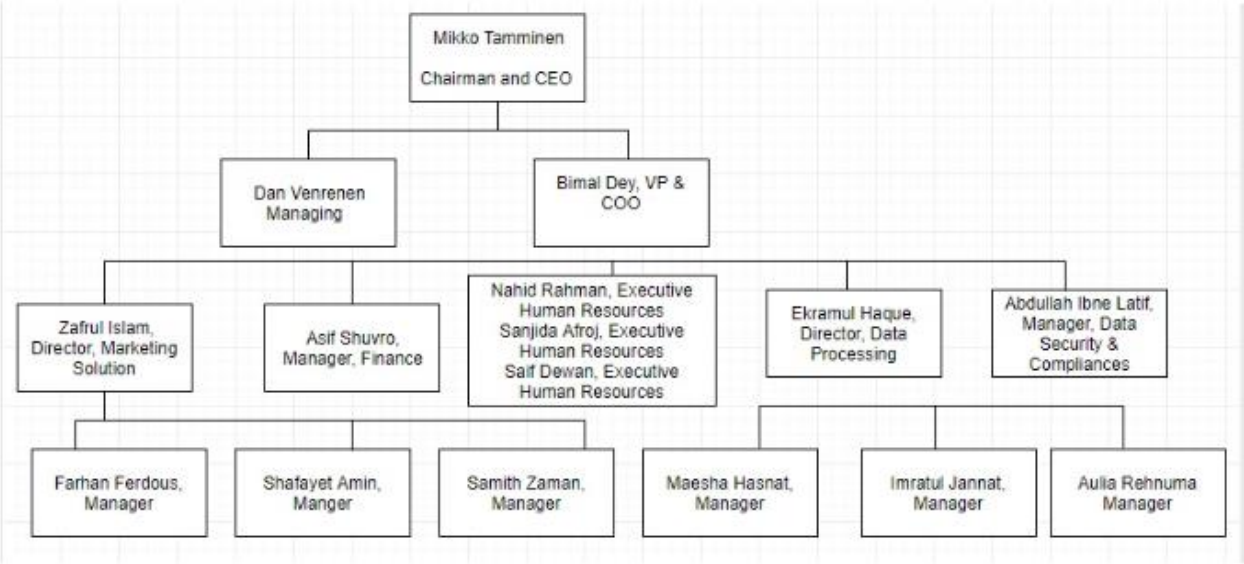
Observed as a company with "friendly environment" and a place where it takes ownership of its own development and outrival in professionalism through creating values for all the stakeholders.

Values that characterize the employees:

- Help each other grow as professionals
- The office is a place to grow professionally and to use the spare time to learn new things which will help to excel
- Learn and improve professionalism through experimenting or failing while experimenting
- Taskeater understands the context of its delivery and how it's creating values for the clients

2.4 Company Organization and Management

The present company organization as of 16 November 2018 is portrayed in the following diagram:



2.5 Services offered

- Lead Generation
- Content Moderation
- Order Processing
- Data-entry
- Tagging and Categorization
- Transcription
- Online Data Collection
- Security Camera Surveillance & Call Centre auditing etc.

Chapter 03: Review of Related literatures

I have consulted four journal papers and one thesis paper, related to my topic and clearly have helped me understand the corners that I could miss if I had not consulted these.

- (Kazemi , "A Survey: Information Security Management System", 2017) has tried to introduce the information security management system along with the types of threatening risks of information systems and also introduced and offered proper ways to maintain information security of each organization and then worked on necessary requirements in order to design information security system and phases of implementing management system of information security.
- (Park, Lee, & Yeo, "Advanced Approach to Information Security Management System Model for Industrial Control System", 2014) said that ISO 27000 series is the international standard ISMS used to protect confidentiality, integrity, and availability of sensitive information. But it is not sufficient for a perfect industrial control system (ICS), so they have tried to pitch a new paradigm of ISMS for ICSs, which will be shown to be more suitable than the existing ISMS.
- (Park, Jang, & Park, "A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance", 2010) said that this study will substantiate the fact that development and certification of ISMS positively affect the business performance of enterprises so that they will recognize the effect of obtaining ISMS certification and eventually prevent security accidents and improve their business performance by developing ISMS.
- (Susanto, Almunawar, & Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five", 2011) have tried to provide a picture of the position and specialization of each information security standard, adoption by countries and their usability levels.
- (Karjalainen, "Developing an Information Security Management System", 2014) in his thesis paper, mentioned that it requires plenty of expertise to gather relevant parts of the legislation in a company to form a functional information security management system.

Chapter 04: Work Experience

I had joined Taskeater Bangladesh Limited exactly on 14th June, 2018 as a fulltime Analyst. Since then, I have worked for five clients, precisely. My primary client's requirements were Business Card Transcription, Events research and Lead Generation. On the other hand, I worked for 9fin, which is basically a website which is used by investors as it contains financial data of numerous companies. My job was to collect financial information of those enlisted companies and prepare financial statements, which were later input in the website of 9fin. Then I have temporarily worked on two clients which were Mixcloud and Doordash. While I had worked for Mixcloud, I did content moderation and for Doordash, I had to prepare Restaurant menus on a regular basis.

Now, I work for Syft. My job there, is to prepare invoices for the workers of this company. This United Kingdom based company basically provides part time employment and my job is to prepare daily invoices for those part time workers so that they get their payment timely and accurately. I need to make sure that my invoices are correct and precise so that no one has to face the hassle of contacting my client and complain about late or incorrect payments.

On another note, I have been working with extremely sensitive information and this is my job to maintain the security and confidentiality of the information that I work with.

Chapter 05: Analysis and Interpretation of the Data

As a BPO company, managing client's manual processes, Taskeater Bangladesh Limited collects, validates, enters, enriches and cleanses information of different types. Laws and regulations, as well as industry standards, also impose obligations on Taskeater to protect confidentiality, integrity and availability of information. Managing these information resources with appropriate safeguard is very crucial to Taskeater and its clients.

Its employees, process and infrastructure forms basis for all its activities, and are essential to services that it is providing to its customers. It recognizes the need for its employees, contractors, service providers and visitors to have access to the information they require in order to carry out their work and recognizes the role of information security in enabling this. Security of information must therefore be an integral part of the management structure in order to maintain continuity of its business, legal and regulatory compliance.

Taskeater Bangladesh Limited understands that information requires protections against risks that would threaten its confidentiality, integrity and availability and therefore recognizes that the disciplines of confidentiality, integrity and availability in Information Security Management are integral parts of its management function and also a framework for classifying information assets and manage and secure the same in regards to the requirements of it's different stakeholders. The management of Taskeater views the seas primary responsibilities and fundamental to the best business practice of adopting appropriate Information Security Controls in line with ISO 27001/2013 standard.

Its Information Security Policy seeks to operate to the highest standards continuously and to implement and operate fully ISO 27001/2013 standard, including continual improvement through process supported in the standards and also through registration and annual review.

Responsibility for upholding this policy is organization-wide under the guidance and with the assistance of the CEO who encourages the personal commitment of all staff to address Information Security as part of their skills.

This policy defines the framework within which information security will be managed across the organization and demonstrates management direction and support for information security throughout the organization. This policy is that the primary policy below that all different technical and security connected policies reside.

This policy is applicable to and will be communicated to all employees, customers and other relevant parties including visitors and contractors. It covers, but is not limited to, any systems or data attached to the Taskeater's computer or networks, systems supplied by the Taskeater, any communications sent to or from the Taskeater and any data held on systems owned by Taskeater.
The information resources (the "Information Resources") included in the scope of the Information Security Policy are:

- All data regardless of the storage medium (e.g., paper, USB, external, drive, hard drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.)
- The computing hardware and software systems that process, transmit and store data
- The Networks that transport data

Taskeater is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for information security and to ensuring the continued business of the services providing to its customers. It is the policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to confirm acceptable legal, regulatory and contractual compliance. To determine the acceptable level of security management that ought to be applied to info systems, a process of risk assessment shall be carried out in order to define security requirements and determine the likelihood and impact of security breaches.
Specialist advice on information security can be sought via the InfoSec Team. It is the InfoSec Team's policy to report all information or IT security incidents, or other suspected breaches of this policy. The InfoSec Team will follow the Organization's advice for the escalation and reporting of security incidents and data breaches that involve personal data will subsequently be reported according to the process. Records of the number of security breaches and their type should be kept and reported on a regular basis and must be accessible for all members of InfoSec Team. Failure to comply with this policy that occurs as a result deliberate, malicious or negligent behavior, may result in disciplinary action.

Classification of Data

Any person WHO uses, stores or transmits information features a responsibility to keep up and safeguard such information. The first step in establishing the safeguards that ar needed for a selected sort of information is to see the extent of sensitivity applicable to such information. Data classification could be a methodology of assignment such levels and thereby deciding the extent to that the info have to be compelled to be controlled and secured.

Data Classification Policy applies to all data owners or data owners on behalf of our clients at Taskeater. Data security measures must be implemented commensurate with the sensitivity of the data and the risk to the Taskeater if data is compromised. It is the responsibility of the applicable data owner to evaluate and classify data for which he/she is responsible according to the classification system adopted by the Taskeater and described below. If information of quite one level of sensitivity exists within the same system or termination, such data shall be classified at the highest level of sensitivity.

Taskeater has adopted the following four classifications of data.

Sensitive data

Any information protected by state or local laws and regulations or industry standards, such as GDPR. Sensitive data include, but are not limited to: Personally Identifiable Information (PII) to comply with GDPR: any information about an individual that (a) can be used to distinguish or trace an individual's identity, such as name, date and place of birth, mother's maiden name or biometric records, (b) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual and (c) is protected by state or local laws and regulation or industry standards. Examples of Pll include, but are not limited to, any information concerning a living person that can be used to identify such living person, such as name, number, personal mark or different symbol, in combination with any one or more of the following:

- Driver's license number or non-driver identification card number (such as, social security number, NID, passport number)
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account

- Email address with password

Name, telephone number, account number, any element of dates (except year) for dates directly related to an individual, including birth date, employment date, discharge date or any other unique identifying range, characteristic, code or combination that allows identification of an individual

- Telephone number
- Certificate/License number
- Vehicle identifier and serial number, including license plate number
- Device identifier and serial number (MAC address)
- Internet Protocol (IP) address number
- Biometric identifier, including finger and voice print
- Full face photographic image and any comparable image

Confidential data

Any information that is contractually protected as confidential by law or by contract and any other information that is considered by the Taskeater appropriate for confidential treatment. Examples of confidential information embrace, but are not limited to:

- Employee records; except "directory information", such as a employee's name, address or other contact information which is required by the team and managers
- Human resources information, such as salary and employee benefits information
- Non-public personal and financial data about employee
- Information on Taskeater's security systems, businesses and strategic plans, client's detail Non-public intellectual property, including invention disclosures and patent applications

Internal data

Any information that is proprietary or produced only for use by Taskeater employees with legitimate access of such data. Examples of Internal information embrace, but are not limited to:

- Taskeater Staff Handbook
- Taskeater's policies
- Internal operating procedures and operational manuals
- Internal memoranda, emails, reports and other documents
- Technical documents such as system configurations and floor plans
- Directory information of our employees

Public data

Any information that is available to the general public, with no legal restrictions on its access or its use. Examples of Public information embrace, however don't seem to be restricted to:

- Data available on www.taskeater.com
- Copyrighted materials that are available to the public

ISMS Scope and Boundaries

Information Security Management system covering Lead generation, data entry, data processing, data collection and data verification, digital marketing and support functions like HR & Training, Facility management, IT infrastructure and Procurement as per SOA 2 dated 26th June 2018.

Takeater's delivery center in Dhaka is divided into 2 business units:

- Marketing Solutions is delivering lead generation, email campaign and digital marketing services to clients outsourced these tasks to Taskeater.
- Data Processing Services is delivering data entry collection/enriching/validation, tagging, content moderation and other data processing services.

HR, Finance and IT are the main supporting functions for these 2 business units. As of 20th May 2018, Taskeater Bangladesh Lid employs 300+ employees.

All business and supporting processes of Taskeater are included within the scope of ISMS. The scope also includes all critical and sensitive Information Assets of Taskeater, including paper documents as well internal IT systems and infrastructure.

The scope covers employees, contractors and service providers who may be bound by contractual agreements. Some hardware assets, software assets, network assets, and utilities, including power supply and internet Service Providers, are the identified resources within the scope, equipment owned by third parties, but in the custody of Taskeater, will also be covered under the scope.

The facilities to be developed below future growth plans, as well as code and alternative IT Systems, can mechanically be enclosed at intervals the scope of ISMS.

Organization of Information Security

Data Security and Compliance Manager is responsible for the main emance of this policy and for compliance within the Taskeater. InfoSec Team comprising senior managements of Taskeater along with Data Security and Compliance Manager has approved this policy. InfoSec Team is responsible for reviewing this policy on an annual basis. They will give clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.

Data Security and Compliance Manager is also responsible for the management of information security and, specifically, to provide advice and guidance on the implementation of this policy. The Information Security Advisory Board comprising line managers from all relevant business units is responsible for identifying and assessing security requirements and risks and supporting InfoSec Team. It is the responsibility of all line managers to implement this policy within their area of responsibility and to ensure that all employees for whom they are responsible are made absolutely attentive to the policy and given applicable support and resources to obey. It is the responsibility of every member of workers to stick to the present policy.

Information security roles and responsibilities

- Executive Management
- Security Management
- Information Security & Compliance Manager
- Asset Owners
- System Ownership
- Technical Ownership
- System or Data Usage

Segregation of duties

Contact with authorities

Contact with specialist interest groups

Information security in project management

Review of the policies for information security

Policies

Human Resource Security Policy

- **Prior to employment**
    - Screening
    - Terms and conditions of employment
    - Communication of terms and conditions of employment
    - Violation of terms and conditions of employment
- **During employment**
    - Supervisor responsibilities
    - Review of security roles and responsibilities
    - Orientation for new employees
    - Ongoing information security awareness, education and training
    - Reviewing security breaches and policy violations
    - Termination of employment responsibilities

Physical & Environmental Security Policy

- Physical security perimeter
- Physical Entry Controls
- Securing offices, rooms and facilities
- Protecting against external and environmental threats
- Working in secure areas
- Delivery and loading areas

Acceptable Use Policy

- General use and ownership
- Security and proprietary information
- Unacceptable use
- System and network activities
- Email and communication activities
- Blogging and social media

Password Policy

- General
- Password selection guidelines

- Password Protection
- Storing the password

Clean Desk Policy

Email Policy

Registration and Protection of Endpoints Policy

- Registration of endpoints
- Deregistration of endpoints
- General protection requirements for desktop and laptop computers
- General protection requirements for mobile devices
- Additional protection requirements for endpoints containing sensitive or confidential data
- Additional protection requirements for endpoints containing sensitive data

Antivirus Policy

Information Resource Access Control and Log Management

- Requirements for system owners and IT custodians
- Password requirements
- Login Requirements
- Log Management
- Remote access

Sanitization and Disposal of Information Resources Policy

- Non-sensitive and non-confidential data
- Sensitive and confidential data

Technology Equipment Disposal Policy

- Technology equipment disposal
- Employee purchase of disposed equipment

Removable Media Policy

Remote Access Policy

- General
- Requirements

Teleworking Policy

- Laptop take-home requirements
- Checking company email remotely

- Expenses from working remotely

Remote Access Tools Policy

Internet Usage Policy

- Internet services allowed
- Allowed usage
- Personal usage
- Prohibited usage
- Review of public information
- Expectation of privacy
    - Monitoring
    - E-mail confidentiality
- Maintaining corporate image
    - Representation
    - Company materials
- Periodic reviews
    - Usage compliance reviews
    - Policy maintenance reviews

Internet Use Monitoring and Filtering Policy

- Website monitoring
- Access to website monitoring reports
- Internet use filtering system.
- internet use filtering rule changes
- Internet use filtering exceptions

Change Management Policy

Procurement Policy

Information Security Risk Management

This policy is to protect the confidentiality, integrity and availability of Taskeater's information resources and to ensure that Taskeater is operating with an acceptable level of risk. Information Security Risk Management covers all of the Taskeater's information resources, whether managed or hosted internally or externally. Executive managers, system owners, data owners and IT custodians are responsible for working with the applicable Information Security Office to implement the information Security Risk Management Program, including remediation of identified risks in a timely manner.

The Information Security Risk Management Program is comprised of the subsequent processes.

Information resources risk categorization

All information resources that store, process or transmit data are included in the policy. Information resources are categorized based on their function, threat exposure, vulnerabilities, and data type pursuant to the data Classification Policy. The categorization method takes under consideration the subsequent elements:

- Size, complexity and capabilities of the information resources and organizations;
- Technical infrastructure, hardware and software capabilities,
- Cost of implementing security controls, and
- Probability and criticality of risks to data, particularly sensitive or confidential data.
- Resources to handle risks are allotted consistent with the known risks.

Security control selection

The appropriate security controls to mitigate known risks are selected supported the character, feasibility and cost effectiveness of the controls. The Taskeater has selected elements from the following security control frameworks to use as part of its Information Security Risk Management framework:

- ISO 27002, Security Techniques - Code of Practice for Information Security Management; and
- ITIL- Industry Standard Framework for IT Service Management Guidelines and Best Practices.

All systems and endpoints must meet the baseline requirements as defined in the Taskeater Registration and Protection of Endpoints Policy and Taskeater Server Security Policy. Additional

controls are going to be evaluated supported the framework outlined on top of and applied supported risk analysis.

Risk analysis

A documented risk analysis method is employed because the basis for the identification, definition and prioritization of risks. The risk analysis process includes the following:

- Identification and prioritization of the threats to information resources;
- Identification and prioritization of the vulnerabilities of information resources;
- Identification of a threat that may exploit a vulnerability;
- Qualitative identification of the impact to the confidentiality, integrity and availability of information resources if a threat exploits a specific vulnerability; and
- Identification and definition of measures and/or controls used to protect the confidentiality, integrity and availability of information resources.

The risk analysis method is updated once environmental, operational or technical changes arise that impact the confidentiality, integrity or availability of information resources. Such changes include:

- New threats or risks with respect to the information resources;
- An information security incident;
- Changes to information security requirements or responsibilities. (e.g., new law or regulation, new role defined in Taskeater, new or modified security controls implemented. etc.); and
- Changes to the Taskeater's organizational or technical infrastructure that impacts information resources (e.g., addition of a new network, new hardware software standard implemented, new method of creating. receiving, maintaining or transmitting data, etc.).

When security measures for AN info resource don't meet a security normal, risks are identified and expressed. Three factors are considered when determining the risk:

- The type of possible threat and its likelihood;
- The extent of effectiveness of current security controls or their vulnerability; and
- The likely level of impact.

Risks are qualitatively expressed as High. Medium and Low. For purposes of this policy, high, medium, and low risks are defined as follows:

- High: The risk of imminent compromise or loss of sensitive data from either external or internal sources or where sensitive data has already been exposed. There is no control in place to protect the data or only a single control, or multiple ineffective controls, in place to protect the data.
- Medium: The risk of compromise or loss of sensitive data is possible from another external or internal sources. Although less likely from external so to protect the data.
- Low: There is no realistic risk of compromise or loss of sensitive data.

Risk Remediation

The methods for risk correction ar proportionate to the risks to the knowledge resource. The selected and enforced risk management measures moderately shield the confidentiality.

Integrity and handiness of data resources and therefore the risk is managed on endless accepted risk is accomplished in a very real incident, the risk analysis and management are repeated with the new information, and re-addressed with greater sensitivity and urgency based on the nature and extent of the incident.

Risk monitoring

The results of Risk. Analysis and Risk Remediation are documented and reviewed by executive managers, the applicable information Security Manager, system owners, data owners and IT custodians. Monitoring processes are used to evaluate:

- The effectiveness of security controls;
- Changes to information resources and environments of operations: and
- Compliance with laws and regulations, industry standards and Taskeater policies.

The frequency of risk observance are going to be based mostly on:

- Regulatory compliance requirements;
- The importance or sensitivity of the information resource;
- The requirements of the information Security Policies; and
- The degrees to which systems are interconnected to one another and the risk posed by such connections.

Data Breach Response Process

The purpose of the policy is to establish a breach response process and to define to whom it applies and under what circumstances, and it will include the definition of a breach, employee's roles and responsibilities, standards and metrics (e. g. to enable prioritization of the incidents). Well as reporting, remediation, and feedback mechanisms. Taskeater is committed to protecting its employees, clients, partners and the company from illegal or damaging actions by individuals: either knowingly or unknowingly.

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle confidential or sensitive data. Any agreements with vendors or partners will have the same liability described in this document.

Reporting of incidents

Errors and other abnormal system behavior can be the indication towards a breach of IT security and therefore should always be reported. It is every employee's responsibility to report any security incidents and weaknesses to the InfoSec Team. InfoSec Team will assess the seventy of the issue and if vertical then report directly to the CEO.

Following are some examples of IT security incidents:

- Stolen equipment or theft of physical IT asset including computers, storage devices etc.
- Loss of information confidentiality (data theft)
- Reports of unusual system behavior. Workstations or the system behaves abnormally, suspecting viruses
- Human errors which affect IT security and violate security policy, such as saving their passwords on shared computer
- An attempt at unauthorized access
- Infection of systems by unauthorized or hostile software
- Compromise of information integrity (damage to data or unauthorized modification)
- Damage to physical IT assets including computers, storage devices, etc.
- Misuse of services, information, or assets
- Unauthorized changes to organizational hardware. Software, or configuration
- Responses to intrusion detection alarms

This policy mandates that any individual who suspects that a theft, breach or exposure of Taskeater confidential or sensitive data has occurred must immediately provide a description of what occurred via email, by calling a designated number, or through the use of reporting page.

The Taskeater's Information Security Team (InfoSec Team) monitors the email box, phone number, and Google reporting page. The team described later in this document will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the InfoSec Team will follow the appropriate procedure in place.

Confirmed breach

As soon as confirmed theft, data breach or exposure of Taskmaster confidential or sensitive data is identified, the process of removing all access to that resource will begin.

The Executive Director are going to be notified of the larceny, breach or exposure. IT, beside the selected rhetorical team, will analyze the breach or exposure to determine the root cause.

The Executive Director can chair an event response team to handle the breach or exposure.

The team will include members from:

- Infrastructure
- Finance
- Legal
- Human Resources
- The affected business unit that uses the involved system or output or whose data may have been breached or exposed

The above team with help of experts will determine how the breath or exposure occurred; the types of data involved; the number of internal external individuals and organizations impacted; and analyze the breach or exposure to determine the root cause. First and foremost the lost data should be identified. The team is required to identify which data has been lost, leaked or in any other way been affected, who are affected, the way in which said people are affected and possible quick solutions they can undertake to prevent any further damage. Furthermore the team should immediately try to determine the cause of the incident, any possible leaks and work to find a solution to repair the cause as well as new measures to ensure that the same accident does not happen again.

Chapter 06: Findings of the Study

Benefits of Adopting ISMS awareness

While carrying out the research, I have found out a few things that I would like to include in this paper. Firstly, the benefits of ISMS awareness within the organization and the interest gained after successful implementation of ISMS and achieving the ISO 27001 certification, are tremendous.

● The potential loss from the possible threat of the current information system operation can be quantitatively predicted and followed up. Administrators and users will perceive the danger level and scale back the danger chance.

● The organization's assets stability, effectiveness, efficiency and reliability can be improved.

● The visual presentation of the risk level through risk analysis and evaluation can inspire the security awareness of the administrators and users.

● It supports decision making to establish the security measures with consideration to priority and cost/effectiveness aspects of the high risk areas.

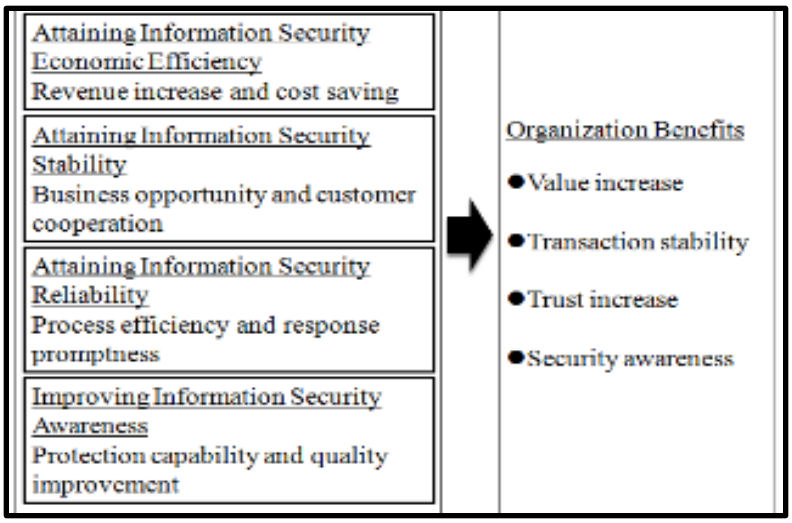
● Certification by the government means that the enterprise is properly managing the information security thus improving public trust and competitiveness.

● The enterprise can notify the users or trade partners that it is complying with the legislation, procedure or guidelines to improve their corporate image.

● The corporate mission and vision of the organization can be met.

However, despite the clear advantages as mentioned on top of, such benefits may not be clearly visible to the enterprises obtaining the certification. Therefore, it's dangerous to rationalize the data security management system certification by victimization typical cost/effectiveness analyses and its additionally troublesome to research and manage the tangible and intangible measurement factors that can be additionally attained.

The following figure will make the above mentioned, clearer.



Now, how Taskeater Bangladesh Limited is getting benefited by being aware about the ISMS is the main focus of mine since the main task is to relate the topic with my organization.

Well, Taskeater is getting the positive vibe already, even though it has not yet got the ISO 27001 certification. There are a few points that I would like to mention, that I have found out by talking to my line manager, finance manager and IT manager, also by talking to my colleagues and from my own observations and understanding.

- Taskeater has never been so secure until now. The data that this organization contains within its premises as well as on its server, is more secure now.
- Because of the recent changes and additions in policies, Taskeater is now more reliable to its clients and other potential clients that it targets to acquire.
- Though the maintenance costs have increased, the risks have been mitigated, for example if anything wrong like Breach of Data even happens, Taskeater now has proper remedies/actions prepared.
- Taskeater has become different than its competitors by adopting the ISMS awareness. This gives the potential global and local clients an additional reason to outsource their business processes to this company.
- Taskeater has acquired more than 500 employees until today even though the number was less than 300, five months ago. This has happened not only because of the good performance that it delivers to its clients, but also the recent ISMS awareness that it has adopted. Because of the change in policies and additions, Taskeater is getting clients like never before and more client results into more workforce.

Nonetheless, Taskeater is getting close to its goals step by step. One day, it might achieve the goals and go for bigger steps. ISMS awareness is a boost to its successful journey and after it

gets the ISO 27001 certification, Taskeater will turn into one of the greatest multinational companies in the outsourcing industry, not only in Bangladesh, but also in the world.

Benefits of ISO 27001 Certification

ISO 27001 is the only auditable international standard that defines the requirements of an Information Security Management System (ISMS). By getting this certification, an organization can claim that it has the best practice of Information Security Processes. The benefits of getting an ISO 27001 certification are as follows:

- Winning new business and sharpening the competitive edge: Being a holder of this certificate, an organization can easily acquire clients without even any sort of verification as they are already internationally verified. Also, a company holding this certification, will surely get better emphasize from the customers than its competitors.
- Avoid the financial penalties and losses associated with data breaches: According to Ponemon, a research institute, the average cost of global data breach has skyrocketed to $3.86M which is a 6.4% increase from the last report of 2017. So, as per the global benchmark of managing information assets effectively, ISO 27001 certification enables organisations to avoid the potentially devastating financial losses by data breaches.
- Protect and enhance reputation: Cyber-attacks are more frequent nowadays. Companies containing valuable information within their serves are more vulnerable to the situation. So, if ISO 27001 certified ISMS is implemented then the organization stays secured and it also demonstrates that the organization has taken proper protection and it is good sign since it helps to acquire clients.
- Comply with business, legal, contractual and regulatory requirements: The standard is basically designed to ensure the selection of enough and proportionate security measures that help to protect information in line with increasingly rigid regulatory requirements such as the EU General Data Protection Regulation and directive on security of Network and Information Systems.
- Improvisation of Structure and Focus: By clearly setting out information security risk responsibilities, this standard helps businesses to be more productive. This is important because efficient businesses grow rapidly and it really does not take long before confusion about responsibility distribution on information assets arises.

- Reduction of Frequent Audits: Once an organization gets the certification, it gets a globally accepted demonstration of being effective in terms of security management. So, the organization will not be needing to go through audits, repeatedly.

The certification of ISO 27001 is a clear indication of an organization being secured. But, the organization still gets audited over time to improve because there will be always a room for improvement. Also, the organization is kept an eye upon, by the auditors, so that it does not lose its focus on ISMS over time. When the organization always gets positive reviews after those audits, done intervally, it gradually obtains a positive image upon itself and it is really a win-win situation for both the company and the clients.

However, at the end of the day, it's all about the returns of the investments. So, it is really important to know if the organization is experiencing the increase in returns from the investments done. Implementing ISMS on the organization's policy, is an investment, to reduce costs. How? Ponemon research institute, backed by IBM, did a research on the global data breach. According to (Ponemon, "Cost of a Data Breach Study", 2018), the global the average cost of a data breach globally is $3.86 million, which is a 6.4 percent increase from year 2017's report. The major costs, caused by Data Breach are:

- Lost businesses
- Negative impact on reputation
- Employee time spent on recovery

These are considered as costs because they impact directly on the finance of the affected organizations. So, Implementing ISMS on the organization's policy is definitely a good measure to reduce costs. Also, it helps an organization to grow financially too. A secured and reliable organization gets greater number of customers/businesses/clients, which brings more revenue and when the Data Breach Costs are reduced, profit increases. Most importantly, terms like ROI, Employee Turnover Rates etc. do show positive percentages over time.

However, I have been working into Taskeater for 6 months and I have seen the changes by myself and Taskeater has never been this big before implementing ISMS on its policy and working hard to get the ISO 27001 certification.

Return on Investment

Investing on anything basically brings out the question of getting the sufficient return to satisfy the judgement. In terms of getting return on investing on the Information Security Management System of the organization, it's really satisfying.

The return on investment in this case is really satisfying because Taskeater Bangladesh Limited is firstly, securing itself like never before. On another note, when it gets the ISO 27001 certificate because of abiding by the rules and standards, it will get more recognition as a secured organization to provide information to, which will bring in more clients and more client means more revenue which ultimately ensures greater profits since the cost of Data Breaches will be at point ZERO by then.

The basic rule of ROI is:

(Gain from Investment - Cost of Investment) / Cost of Investment

But in this case, calculation of ROI is a bit different. Firstly, Annual Loss Expectancy has to be calculated. The formula is to multiply Number of Incidents per Year with Potential Loss per Incident.

After that, to calculate the ROI, formula goes as: ROI = [(ALE / Cost of Countermeasures) x 100%].

After calculation of the ROI, the percentage that any organization would get, is actually less than the greater outcomes that cannot be calculated. The returns are much more than the percentage as far as I have seen the consequences here at Taskeater Bangladesh Limited.

Chapter 07: Recommendation & Conclusion

Taskeater Bangladesh Limited went through its first audit to get the ISO 27001 certification on September 18, 2018. According to the audit team, we still have some lacking. I had talked to my supervisor to find out what were the points that the audit team had raised. She shared a few ideas. So, from those findings and my own opinion, I am going to recommend some of the points that Taskeater might work on so that they get the certification after the second audit which is going to happen soon.

- Improve working space for sensitive data related task: Since Taskeater has an open work space, it is really hard to maintain the confidentiality within the employees of the organization. However, this is a requirement that Taskeater needs to work on, so that they can successfully maintain the confidentiality of information and boost up their way to getting the ISO 27001 certification as well.
- Improve in house surveillance system: Improving the in house surveillance system in a workplace like Taskeater is very hard but not impossible. They should be using more security cameras, people to monitor.
- Improve logs/tracking of device and their users: Taskeater does keep the logs and tracking of the devices that are owned by the organization, but it was not that much important until today since Taskeater is now aware about the requirements of getting the ISO 27001 certification.

So, these are the most important points that Taskeater Bangladesh Ltd. needs to work on. Otherwise, all these efforts of months will go in vein both in terms of getting the ISO 27001 certification and efficient ISMS as well.

Reference

- Kazemi, U. (2017). A Survey: Information Security Management System. Journal of Analog and Digital Devices, 2(3), 1-6. Retrieved December 2, 2018, from https://www.researchgate.net/publication/322569424_A_Survey_Information_Security_Management_System.
- Park, S., & Lee, K. (2014). Advanced Approach to Information Security Management System Model for Industrial Control System (S. Yeo, Ed.). The Scientific World Journal, 2014, 1-13. http://dx.doi.org/10.1155/2014/348305
- Park, C., Jang, S., & Park, Y. (2010). A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance. International Journal of Computer Science and Network Security, 10(3), 10-21. Retrieved December 2, 2018.
- Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences IJECS-IJENS, 11(5), 23-29. Retrieved December 2, 2018, from https://www.researchgate.net/publication/228444915_Information_Security_Management_System_Standards_A_Comparative_Study_of_the_Big_Five.
- Karjalainen, M. (2014). Developing an Information Security Management System (Unpublished doctoral dissertation). Laurea University of Applied Sciences. Retrieved December 2, 2018, from https://www.theseus.fi/bitstream/handle/10024/79945/Mika ONT 18 5 2014.pdf?sequence=1.
- Schneier, B. (2008, September 02). Security ROI: Fact or Fiction? Retrieved from https://www.csoonline.com/article/2123096/metrics-budgets/security-roi--fact-or-fiction-.html
- Marks, N. (2018, July 18). Is There an ROI for Investing in Information Security? Retrieved from https://www.cmswire.com/information-management/is-there-an-roi-for-investing-in-information-security/

- Return on Investment (ROI) of Information Security – What Business should consider? (n.d.). Retrieved from https://www.linkedin.com/pulse/return-investment-roi-information-security-what-should-pranjale
- Return on Investment (ROI) – A Touchy Security Topic. (n.d.). Retrieved from https://zeltser.com/touchy-security-topics-roi/
- Kolochenko, I., & IDG Contributor Network. (2015, December 01). How to calculate ROI and justify your cybersecurity budget. Retrieved from https://www.csoonline.com/article/3010007/advanced-persistent-threats/how-to-calculate-roi-and-justify-your-cybersecurity-budget.html
- The benefits of implementing an information security management system (ISMS). (n.d.). Retrieved from https://www.itgovernance.co.uk/isms-benefits
- Information Security Strategy – 3 Benefits and 3 Implementation Tips. (2018, September 18). Retrieved from http://www.proserveit.com/information-security-strategy/
- Risk Management & Information Security Management Systems. (2016, January 20). Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms
- Islam, M. Z. (2018, February 03). BPO sector showing signs of promise. Retrieved from https://www.thedailystar.net/business/bpo-sector-showing-signs-promise-1529644
- Correspondent, S. (2018, April 15). BPO Summit 2018: Outsourcing firms eye 1 lakh jobs in 3 yrs. Retrieved from https://www.thedailystar.net/frontpage/bpo-summit-2018-outsourcing-firms-eye-1-lakh-jobs-3-yrs-1563157