INTERNSHIP REPORT ON

"Information Security Management Systems (ISMS) and Categorization of Data: Enhancing Awareness"

Imam Hossain Shanto

This report is submitted to the school of Business and Economics, United International University as a partial requirement for the degree fulfillment of Bachelor of Business Administration.

INTERNSHIP REPORT

Submitted to:

Ahmed Imran Kabir

Lecturer

School of Business & Economy

United International University

Submitted by:

Imam Hossain Shanto

ID: 111182112

Date of submission: 2nd April, 2023

Letter of Transmittal

2nd April, 2023.

Ahmed Imran Kabir
Lecturer
School of Business & Economics
United International University

Subject: Submission of internship report on “Information Security Management Systems (ISMS) and Categorization of Data: Enhancing Awareness” at AMCO Enterprise Limited”.

Dear Sir,

I respectfully wish to inform you that I have successfully completed my internship report, and I would like to express my profound appreciation for your invaluable support and guidance throughout the entire term in preparing this report. Without your assistance, the process would have been much more difficult for me. As a part-time employee at AMCO Enterprise Limited, I had the opportunity to gain a comprehensive understanding of the company's operations, an experience I may not have had as an intern.

The report I have prepared includes a concise overview of data classification and the information security management system (ISMS), as well as an examination of the organization's adherence to these systems and the efficiency and effectiveness of their maintenance. I gathered the necessary information from structured and unstructured interviews, a range of periodicals, and relevant websites.

I have diligently followed the instructions you provided, and I hope this report meets your expectations and standards. Thank you for your support.

Sincerely,

Imam Hossain Shanto
ID: 111182112

Letter of Endorsement

That is to certify that Imam Hossain Shanto is a student of United International University, ID: 111182112, Major in Management Information System, has successfully completed his "Internship program" entitled "Information Security Management Systems (ISMS) and Categorization of Data: Enhancing Awareness" at AMCO Enterprise Limited under my supervision.

I have carefully monitored his endeavors to complete this report, which is required for him to pursue his BBA from United International University's School of Business and Economics.

He has implemented everything in accordance with my directions and has done it as resources effectively and efficiently as possible. I believe that this programme will help him build his profession in the future.

I, hereby, acknowledge his work & wish him all the success.

Signature

……..……

Ahmed Imran Kabir

Lecturer
School of Business & Economics
United International University

Acknowledgement

I would like to begin by extending my gratitude to the All-Mighty Allah for making it possible for me to complete the report ahead of time. My most profound gratitude goes out to Ahmed Imran Kabir Sir, whom I hold in the highest regard and who has been both my supervisor and my mentor. Over the course of my studies, he was an invaluable resource in terms of providing me with motivation, direction, helpful suggestions, compassionate counsel, and enthusiastic support.

My superiors, coworkers, Team leader at Amco Enterprise Limited were quite helpful to me right from the start. They provided me with advice, responded to my questions, and gave me assistance with a variety of documents and materials. I would like to take this opportunity to thank Mohammad Anamul Hoque, the Managing Director of Amco Enterprise Limited. I would also want to express my appreciation to the HR executives, who, in a very short amount of time, were able to provide me with the information of which I was in desperate need. I would want to extend my gratitude to the entire Amco family since they have always been there for me whenever I have required their assistance. Because of their engaged response to each and every one of my concerns and inquiries while I was at the office, this journey turned out to be a successful one.

It was an honour and an opportunity for me, and I am very appreciative to have had the chance to work with such a lovely group of people. In conclusion, I would want to express my gratitude to my family, friends, teachers, and coworkers who were there for me anytime I required assistance.

Executive Summary

This report presents an overview of the research conducted during my tenure as an Analyst at Amco Enterprise Ltd., focusing on Information Security Management Systems (ISMS) and Data Categorization: Enhancing Awareness within the context of Management Information Systems (MIS). My interest in the IT sector motivated me to select MIS as the subject of investigation. The report commences with an introduction to the problem and the organization for which I am currently employed. Subsequently, a concise explanation of how Amco Enterprise Ltd. has implemented ISMS awareness and Data Classification procedures to safeguard both its own and its clients' data is provided. In the latter part of the report, the study's effectiveness and efficiency are examined. It should be noted that this report does not encompass all pertinent information, as my organization is committed to preserving the confidentiality of sensitive data. Nevertheless, as a full-time employee, I have endeavored to gather and incorporate as much relevant material as possible into my research.

Contents

Letter of Transmittal 3

Letter of Endorsement 4

Acknowledgement 5

Executive Summary 6

Chapter 01: Introduction 1

1.1 Analysis of the Business Process of Outsourcing 1

1.2 Information Security Management Systems (ISMS) and Categorization of Data. 2

1.3 Objectives of the study. 2

1.4 Scope of the study 3

1.5 Methodology of the Study 3

1.6 Limitation 5

Chapter 02: Company Overview 6

2.1 Company Analysis: 6

2.2 Company vision: 7

2.3 Company mission: 7

2.4 Management Hierarchy: 8

2.5 Service offered: 9

2.6 SWOT analysis: 10

Chapter 03: Related Literature review 11

Chapter 04: Internship Experience 12

4.1 Position, Duties, and Responsibilities 12

4.2 Contribution to Departmental Functions 13

4.3 Evaluation 13

4.4 Skills Applied 13

4.5 New skills developed 14

4.6 Application of academic knowledge 14

Chapter 05: Data Evaluation and Interpretation 14

5.1 The Sorting and Categorizing of Data 16

5.2 Scope of ISMS: 19

5.3 Handling of the Risks Associated with Information Security: 23

5.4 System for Responding to Data Breaches: 27

5.5 Confirmed violation: 29

Chapter 06: Findings of the Study 29
6.1 Advantages of Embracing ISMS Awareness: 29
6.2 Advantages of Obtaining an ISO 27001 Certification 32
Chapter 07: Recommendation & Conclusion 34
Chapter 08: Appendix: 36
7.1 References 36
7.2 Questionnaires: 37
7.3 Progress Report 38

Chapter 01: Introduction

1.1 Analysis of the Business Process of Outsourcing

To comprehend this internship report thoroughly, it is necessary to provide a brief overview of Business Process Outsourcing. BPO is a methodology that involves delegating various business-related tasks to external vendors. Initially, BPO was primarily associated with manufacturing entities, such as soft drink producers, who outsourced significant portions of their supply chains.

However, in the present day, a vast array of services are outsourced. Business Process Outsourcing is typically used by companies to handle either their back- or front-office tasks. Accounting, information technology (IT), human resources (HR), quality assurance (QA), and payment processing are all examples of back-office (or internal business) tasks that businesses might choose to have performed by another company.

Along the same way, front-office services like customer helping line, advertising, and sales can all be outsourced. In addition, organisations may choose to outsource some services, such as payroll, rather than the entirety of a particular functional area.

Business Process Outsourcing was introduced in Bangladesh for the first time in 2008, and the sector increased by 20 percent year-over-year to around $300 million last year, according to industry insiders. This growth was fueled by a few government services. According to Towhid Hossain, the secretary general of BACCO, the local market is enormous and will soon surpass $1 billion (Islam, 2019).

Bangladesh has been endeavoring to be a credible competitor in the BPO, but sadly enterprises at Bangladeshi are only capturing $180 million of the $500 billion in the global outsourcing market. The government has established a powerful committee to assist the outsourcing business in achieving its export goals (Islam, 2019).

1.2 Information Security Management Systems (ISMS) and Categorization of Data.

Companies that deal with sensitive information now recognise the need of data categorization as an integral part of their operations. The administration of data is considerably aided by organising the data according to a variety of criteria. In addition, the development of Information Security Management Systems (ISMS), has been of tremendous assistance to businesses who are in control of sensitive data or that outsource valuable information. ISMS essentially specifies the actions that need to be implemented inside an organisation in order to appropriately protect the confidentiality, availability, and integrity of its assets against potential risks and vulnerabilities (Mistra, 2019). Amco has, to an excellent degree, protected both the private information it maintains on its servers and the servers itself.

1.3 Objectives of the study.

These are the objectives of this study:

Primary Objectives:

The major purpose is to complete the academic internship report, which is a requirement for the completion of the BBA program. This internship is worth three credits in order to comprehend the academic implications of the lessons learned. I attempted to identify the many employment applications of MIS knowledge and skills based on what I've learned from the Management in Information System classes and the BBA degree as a whole.

Secondary Objective:

As secondary objectives, I have concentrated on comprehending the following:

• Understand the ways that AMCO Enterprise Ltd has utilised throughout time for safeguarding its information and classifying its data, as well as the efficacy and efficiency of the Information

Security Management Systems Awareness inside the firm, as well as the benefits that have resulted.

• Understand the difficulties and possibilities that the department encounters on a daily basis.

• How technology plays a part in Amco's BPO

• Function of the analyst at Amco

Overall acquiring a 360-degree understanding of the different department along with its challenges and opportunities in the future globe was the secondary purpose behind the completion of this internship.

1.4 Scope of the study

This internship report focuses on two topics: data classification and information security management system and enhancing awareness as they apply to Amco Enterprise Ltd. The report is founded not only on findings from research, but also on the information, skills, and experience has acquired from working as an analyst for the business and studying Management Information System (MIS).

1.5 Methodology of the Study

This comprehensive internship report showcases the learning outcomes derived from my work experience during my time at Amco Enterprise Limited. It is based on an analysis of the data and information gathered from the job experience and research. The methods for data collection, sampling, and analysis are detailed below:

Data Types:

As the report primarily relies on information from job experience and academic knowledge, the primary data was predominantly utilized. However, secondary data was also used to grasp the organization's historical background and the industry landscape.

- Primary sources:
    - On-the-job practical experiences.
    - Direct discussions with the Department Head, senior executive, and department executives. During these conversations, I used a prepared questionnaire to ask questions during work breaks to gain a deeper understanding of their work, culture, processes, challenges, and suggestions. These discussions provided qualitative data for this study.
    - Personal observations and learnings from the job contributed to a broader understanding of various aspects of the study.

- Secondary sources:
    - Websites containing information on Amco Enterprise Limited’s history and an overview of its evolution over time.
    - Previous research on the BPO sector, and Amco Enterprise Limited.
    - Relevant articles on the subject offered insights into the findings and opinions of different authors worldwide.
    - Other related publications aided in identifying the study's scope.

Sample Size:

Qualitative interviews were conducted with three key members of the Amco Enterprise Limited: the Department Head, the senior executive, and an executive from the same department.

Sampling Technique or Procedure:

The analytics department consists of a team of five members, including two interns, one executive, one senior executive, and one Department Head. The sample was selected to maximize data collection, comprising one executive, one senior executive, and the Department Head. The chosen executive was the most experienced team member, allowing for insight into past and present working procedures. The senior executive, acting as the team leader, provided information on daily operations, while the Department Head offered a broader perspective on the department's opportunities and challenges.

Data Collection Process:

A questionnaire containing open-ended and closed-ended questions was prepared to gather data from various viewpoints. Over the three-month internship period at Amco Enterprise Limited, questions were asked at different times according to the situation. This allowed for a more extended study period and sufficient time to understand and learn throughout the internship. This process enabled the easy identification and monitoring of extensive data, including opportunities, challenges, past solutions, and future possibilities and work scope.

Data Analysis Technique:

Since the data collected was qualitative, various perspectives were obtained for each question. Answers were analyzed by examining provided reading materials, on-the-ground knowledge, and historical trends. The report presents the interviewees' views supported by data from the study.

1.6 Limitation

Throughout my entire internship, my peer colleagues were so supportive to help me learn through the job. Yet there were a few limitations I faced to prepare the entire report. They are as follows:

- Data Confidentiality and copyright issues created barriers to freely conducting the study.

- The BPO & Analysis department is comparatively new to other departments at Amco Enterprise Limited, so I faced a lack of sufficient data availability.
- Conducting such a study within limited days is relatively difficult. A little more time would add more useful insights to my study.

However, I tried to utilize the maximum resources I could avail to complete this study successfully and outline the activities at Amco Enterprise Limited.

Chapter 02: Company Overview

2.1 Company Analysis:

Amco Enterprise Limited is a private limited company located at 56, Kamal Ataturk Avenue, Banani, Dhaka, Bangladesh. The company specializes in assisting the migration of the workforce from Bangladesh to foreign countries. The company serves as a platform for job seekers to view available job opportunities and submit their resumes for consideration. The company also offers HR assistance, job possibilities, recruiting solutions, trade testing, and training services to its clients.

Amco Enterprise Limited has established itself as a reliable and trustworthy partner for clients who seek to fulfill their workforce requirements. The company has built a reputation for providing professional, transparent, and ethical services. The company's focus on building specialized teams to work directly with clients has allowed it to provide personalized services that cater to each client's unique needs.

Amco Enterprise Limited's clientele come from various countries, including Qatar, the United Arab Emirates, the United States of America, Malaysia, Iraq, Bahrain, Oman, and Brunei, among others. The company's services have enabled its clients to fulfill their workforce needs and aid in their development and expansion.

The company is a member of the Bangladesh Association of International Recruiting Agents (BAIRA), the Dhaka Chamber of Commerce & Industries (DCCI), and the Association of Travel Agents of Bangladesh (ATAB). These memberships allow the company to stay up-to-date with industry news and regulations, participate in relevant events and conferences, and network with other professionals in the industry.

Amco Enterprise Limited's bankers include Eastern Bank Limited (EBL) and Social Islami Bank (SIBL), which allows the company to efficiently and securely manage financial transactions related to its recruitment services.

Overall, Amco Enterprise Limited has demonstrated a strong track record of success in the international recruitment and placement industry, with a focus on providing professional and ethical services that cater to each client's unique needs. The company's memberships, partnerships, and commitment to its clients and job seekers have allowed it to establish itself as a reliable and trustworthy recruitment agency in Bangladesh (Amco Enterprise Limited company profile, n.d.).

2.2 Company vision:

The company's vision is to uphold its commitments and remain dedicated to assisting clients in achieving their goals by enabling them to concentrate on their strengths. The aim is to foster long-term and fruitful relationships based on trust, integrity, professionalism, and exceptional service with clients. The company is committed to providing the highest quality employment services to maintain outstanding customer satisfaction.

2.3 Company mission:

The company's goal is to establish itself as the go-to choice for job seekers as well as employers who are looking for an international recruitment consultancy by providing recruitment services of the highest possible quality and establishing itself as the preferred option in both of those categories. The goal is to provide customers with the finest quality service possible while also giving equal weight to the requirements of companies and those looking for work.

Company culture and values:

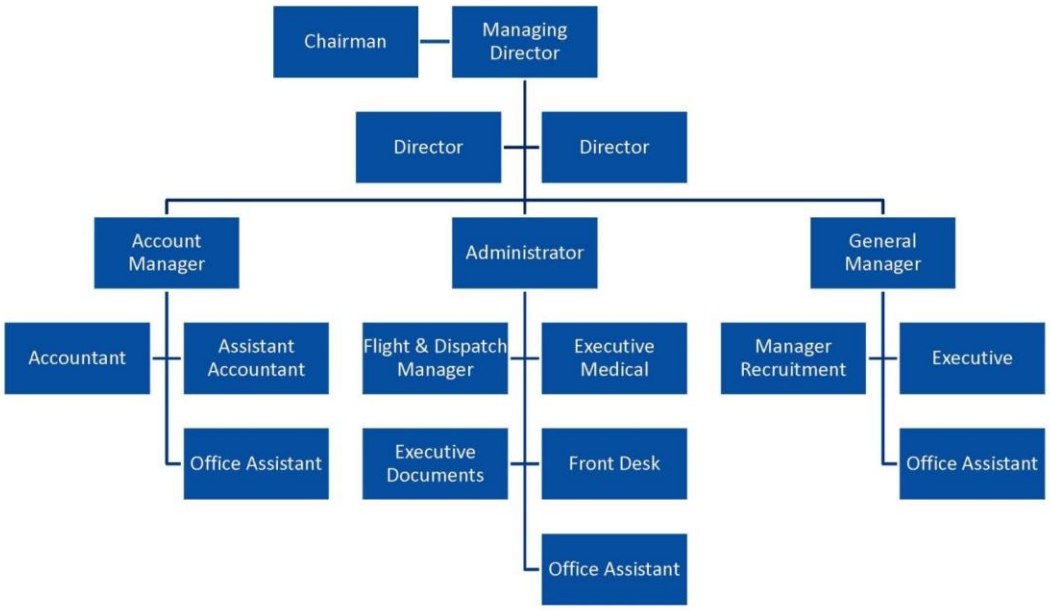
The organisation is renowned for establishing a pleasant work atmosphere, assuming responsibility for its own growth, pursuing professional excellence, and producing value for all stakeholders.

The staff members represent the following values:

- Fostering each other's professional development
- Seeing the job as a growth opportunity and utilising free time to gain new abilities
- Accepting risk and learning from setbacks to enhance professionalism
- Understanding the significance of providing clients with value in context.

2.4 Management Hierarchy:

The following diagram represents the current hierarchy of the organization as of 23rd March 2023:



Important Departments of Amco Enterprise Limited:

Depending on the breadth and difficulty of the goal, each division inside a corporation is indispensable. In their own strategies, the divisions aim for efficacy from their perspective. Departments are staffed with a variety of skilled individuals in order to achieve the company objective more effectively. Amco is a global corporation; thus, each department's activities are planned and executed in accordance with the criteria established by Amco Enterprise Ltd. These are Amco's primary departments:

Commercial	Graphics Design
Finance	Issue and Resolution
Marketing	Content Management
Accounting	Public Relation
Human Resource	Information Technology
Sales Management	Category Management
Business Development	Operations
Administration	Customer Services

2.5 Service offered:

- Pre-selection process
- Selection and deployment process
- Web Based workers Management System
- Validation of Proper Documentation
- Ticketing and Emigration
- Repatriating

2.6 SWOT analysis:

A SWOT analysis examines a company's strengths, weaknesses, opportunities, and threats by examining its marketing strategy and products as a whole or by specific departments (SWOT). It enables a company to make better decisions and achieve greater success in all of its endeavors. The following SWOT analysis of Amco Enterprise Ltd. has been completed.

1. **Strengths:**

Amco Enterprise Limited offers a comprehensive range of services to its clients, including HR assistance, job opportunities, recruitment solutions, trade testing, and training.

The firm establishes specialized teams that work directly with clients, allowing them to outsource certain tasks and concentrate on their core competencies.

The company has a diverse clientele from several nations, indicating that it has established a strong reputation for being a dependable partner in meeting workforce needs.

2. **Weaknesses**:

The company's reliance on foreign markets may expose it to economic and political instability, which may adversely impact its operations.

There may be increased competition in the labor migration services industry, which may pose a challenge to the company's growth.

The company's services may be reliant on the availability of employment opportunities in foreign countries, which may be subject to fluctuations.

3. **Opportunities:**

The company may expand its operations to other countries and regions, tapping into new markets and increasing its customer base.

The demand for labor migration services is expected to increase due to globalization, creating opportunities for the company to expand its services and meet the growing demand.

The company may diversify its services to include other areas such as immigration and settlement services.

4. **Threats:**

The company may face regulatory challenges and compliance requirements when operating in foreign markets, increasing its costs and limiting its operations.

The company may be subject to currency exchange risks, which may impact its profitability and financial stability.

Changes in immigration policies and regulations in foreign countries may negatively impact the company's operations and revenue.

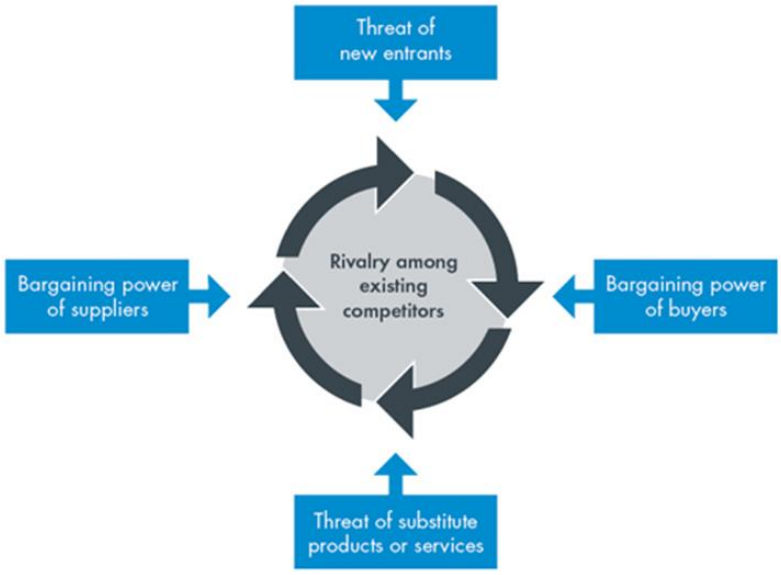


Figure: SWOT Analysis

Chapter 03: Related Literature review

The following is a summary of the few research papers I read that were really helpful in my understanding of the topic.

- The article "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001" evaluates ISO 27001-based ISMSs. The

authors present a case study of a significant financial organisation that adopted an ISO 27001-based ISMS, which improved information security procedures and reduced security incidents. Monitoring and measuring an ISMS's efficacy and efficiency is emphasized throughout the paper. For enterprises seeking an ISO 27001-based ISMS, the paper provides helpful guidance (Boehmer, 2008).

- The article "Information Security management: A human challenge?" examines how difficult information security management is. Information security necessitates acknowledging that employees have personal and social identities in addition to their professional identities. Companies must balance these identities with corporate goals. The article concludes that the human challenge of information security management has been neglected and suggests that addressing this issue requires developing skills to change organisational culture. Ultimately, the essay highlights the relevance of human factors in information security management (Ashenden, 2008).
- The article "Information Security Management System Standards: A Comparative Study of the Big Five (Heru Susanto, 2011)" have tried to provide a picture of the position and specialty of nearly all the information security standard, as well as its acceptance by governments and its degree of use.

Chapter 04: Internship Experience

4.1 Position, Duties, and Responsibilities

As an intern with Amco Enterprise Limited, I was responsible for a variety of tasks. Other from executing the duties that were given to me by the trainers, the obligations I had as an intern were not very challenging. I had a few simple chores to accomplish at the start of training. My trainer would often need me to write a report on previous work and then give me excel figures for inspection. I attended their team meetings and took notes on programme details. They then allocated a project based on client needs, such as software input from plan papers. I kept the excel file updated to ensure the chain of events went well. To avoid having to contact my customer about missing information, I had to make sure my work was exact and precise.In addition, I've been handling very sensitive data, and it was my responsibility to keep it confidential.

4.2 Contribution to Departmental Functions

The Business Process Outsourcing Department is responsible for delegating tasks based on the strategy to the entities that fall under that department. I was assigned to work with a team. The routine tasks that were required of me included:

• Investigating the needs of potential customers

• Input the information in software

• Checking the availability from company's software

• Verification of the client's documentation

• Resolution of any note difficulties

• Evaluation of all contributions

• Import of financial data into software

4.3 Evaluation

Amco Enterprises ensures that every job follows the appropriate procedures. In a team leader assigned tasks based on the client requirements platform and nominated a task reviewer. If no errors are found, the work will be sent to another department for further processing. The organization's software programme logs each task. A team leader assigned this grade to each task in this manner.

4.4 Skills Applied

Throughout the time that I spent serving as an intern at Amco Enterprise Ltd, I put these talents to use.

• Managing time effectively

• Possessing good manners while asking questions

• Communication skills

• Demonstrating a modest demeanor around others

• Technological skills

4.5 New skills developed

My time spent working at Amco Enterprise Limited has equipped me with a very useful expertise. There has been a significant amount of instruction on how to operate the software and how to find solutions to a wide variety of issues. These abilities have contributed in some way to the worth of my future professional life. Learning Excel in particular ahead of time was a very valuable investment.

4.6 Application of academic knowledge

Considering my major was MIS, I was given the opportunity to work at Amco Enterprise Limited, where the entire task was computerized. Easy data collection software apps were utilized by me. After that, I worked on live planning projects in the BPO department. Hence, gained knowledge of some work procedures and data collection software. Several application software was utilized for plan processing and project administration. I performed client-server operations for the client from a Remote Desktop workstation. As my major was in MIS, I was able to effectively operate software applications.

Chapter 05: Data Evaluation and Interpretation

Amco Enterprise Limited controls the manual processes of its clients by collecting, verifying, storing, enhancing, and clearing data. Moreover, Amco Enterprise Limited must protect

information in accordance with laws, regulations, and industry standards. Amco Enterprise Limited and its customers rely on secure data handling.

Amco Enterprise Limited acknowledges that information requires protection against threats to its privacy and security, integrity, and accessibility, and that the safeguarding measures, integrity, and competence in frameworks for categorising information assets and information security management are essential to its function of management and managing and securing them in accordance with stakeholder needs.

Under the guidance of the CEO, every employee must commit to information security as part of their capacity to uphold this regulation. This policy lays the groundwork for managing information security throughout the organization and demonstrates management support. Under this policy, all technical and security policies fall. This policy covers all workers, customers, visitors, and contractors.

Fig: Evaluation and Interpretation (Takieldeen, 2019)

Information and information systems of Amco Enterprise Ltd. are protected. To keep its services operational, it also supports information security education, training, and awareness. It safeguards the information it manages to avoid breaches of confidentiality, integrity, or availability and to maintain legal, regulatory, and contractual compliance. By determining what measures of

protection are needed and estimating the likelihood and impact of security breaches, a risk assessment may determine the optimal degree of security management for information systems.

The InfoSec Team is available to provide specialized counsel on matters pertaining to the protection of information. It is the policy of the Information Security Team to report any event involving information or IT security, as well as any other suspected violations of this policy. The Information Security Team shall adhere to the Organization's recommendations for the escalation and reporting of security events, and any data breaches that include compromised personal information will thereafter be notified in accordance with the procedure. All members of the InfoSec Team need to have access to records detailing the number of security breaches that have occurred as well as the type of breach that has occurred. These records should be retained and reported on a regular basis. It is possible for disciplinary action to be taken against an individual if they are not in compliance with this policy as a consequence of intentional, negligent, or negligently causing activity.

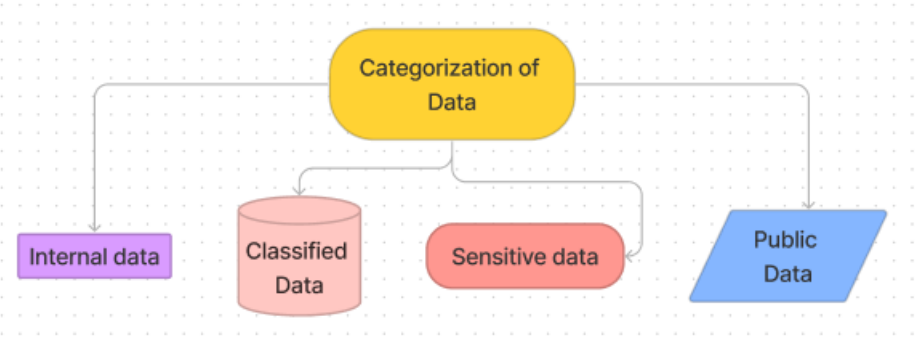
5.1 The Sorting and Categorizing of Data

Each anyone who makes use of information, maintains information, or transmits information has the obligation to keep such information up to date and secure. Finding out the level of sensitivity that is associated with a certain category of information is the first thing that has to be done in order to determine what kinds of protections are required for that information. The assignment of such levels and the subsequent determination of the extent to which the information has to be compelled to be managed and secured can be accomplished through the process of data categorization.

At Amco, the Data Classification Policy is applicable to any and all data owners, including data owners acting on behalf of our customers. It is necessary to establish data security measures that are proportionate both to the importance of the data in question and to the potential damage that might be caused to Amco as a result of its loss. It is the duty of the appropriate data owner to review and categorize the data for which he or she is accountable in accordance with the categorization system that was chosen by the Amco and is stated further down in this article. If

there is information that is significantly different in terms of its degree of sensitivity included inside the same system or termination, then that information must be classified at the most sensitive level possible.

Amco has decided to use the following categories to classify its data.



5.1.1 Sensitive data:

Data that is protected by federal, state, or local authorities, or by voluntary established criteria like the General Data Protection Regulation. The following are some instances of confidential data, however this list is by no means complete:

"(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Any information pertaining to a living person that may be used to identify such a living person, such as a name, number, personal mark, or different sign, in conjunction with any one or more of the following:

- The number on driver's license or identity card if the person is not a driver (such as, social security number, NID, passport number)
- Account number, credit or debit card number, in addition to any requisite security code, access code, or password that, when combined, would allow access to an individual's bank account.
- Email address with a password.
- Name, phone number, account number, any part of a date (except the year) that is directly related to a person, such as birth date, date of employment, date of discharge, or any other unique range, characteristic, code, or combination that can be used to identify a person.

- Phone 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 identifiers, such as fingerprints and voice prints Full face photographic image and any similar image. (Guide to Identifying Personally Identifiable Information (PII), n.d.)”

5.1.2 Classified data:

All information that is legally protected as private or that is protected as secret by contract, in addition to any other information that the Amco Enterprise Ltd. believes should be treated in a confidential manner and that is deemed appropriate for such treatment by the Amco Enterprise Ltd.

5.1.3 Internal data:

Any information that is confidential or created only for use by workers of Amco Enterprise who have the appropriate authorization to access such data.

5.1.4 Public data:

The term "public information" refers to any and all information that is available to the general public and does not have any legal restrictions imposed on either its access or its usage in any way whatsoever.

In accordance with SOA 2 dated June 26, 2018, the Information Security Management System (ISMS) encompasses a wide variety of operations, including data entry, processing, collection, and verification. It also includes digital marketing and support operations, such as HR and Training, Facility Management, IT infrastructure, and Procurement.

5.2 Scope of ISMS:

At Amco Enterprise, the scope of ISMS encompasses not only all business and supporting operations, but also information assets that are both vital and sensitive in nature. Paper records, as well as the company's own information technology (IT) systems and infrastructure, are included in these assets. Under the context of this section, "service providers" includes employees as well as independent contractors and other service providers who may be bound by legal arrangements. There are recognized resources that fall within the scope of this project. These include certain pieces of hardware, software, and network infrastructure, as well as utilities like power supply and internet service providers. Moreover, the scope will extend to cover any third-party property that is in the care of Amco, even if it is owned by someone else. In addition, future expansion plans for facilities, code, and alternative IT systems will be incorporated within the ISMS's scope of work.

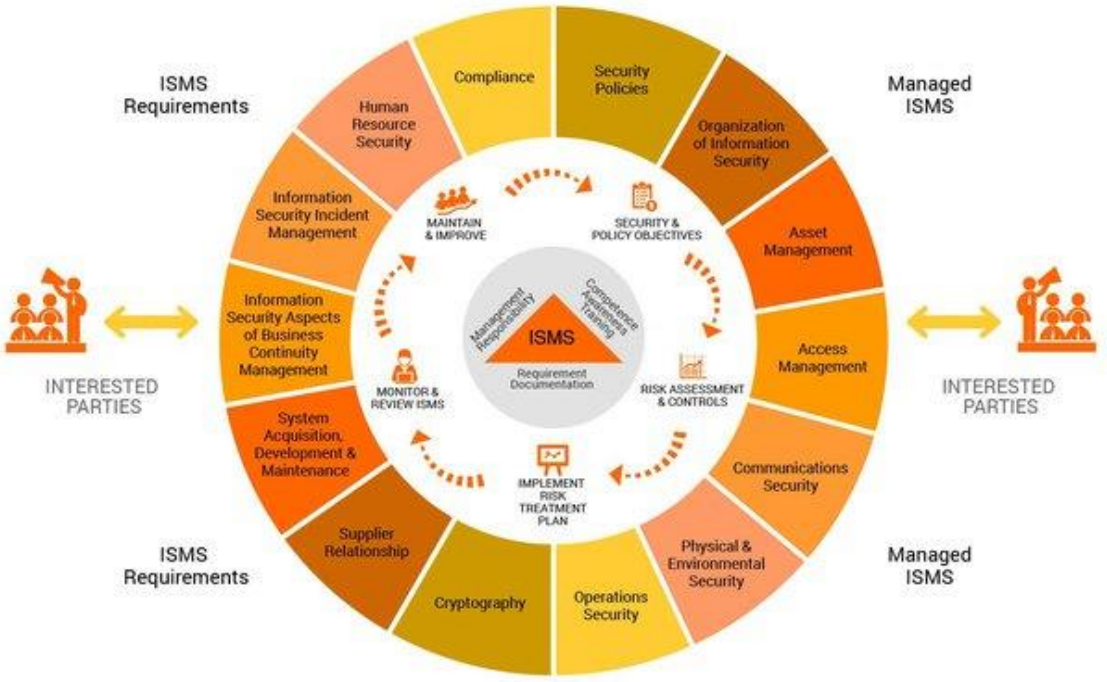


Fig: ISO 27001:2013 (ISO/IEC 27001 Information Security Management System, n.d.)

Information Security of the Organization:

The Data Security and Compliance Manager at Amco is responsible for ensuring that all policies are followed and enforced. The Information Security and Safety Manager oversees information security and provides guidance on how best to put policies into action. Team's ability to determine

and evaluate security needs and threats is greatly enhanced by the Information Security Advisory Panel, which is comprised of supervisors from all important business units. Supervisors are responsible for enforcing this guideline within their respective jurisdictions and making sure their direct reports are aware of and equipped to implement it. The policy is binding for all employees. The tasks and duties involved in information security:

- Property Holders
- Safety administration
- Information Security Regulatory Manager
- Executive Management
- Control of the System
- Authority Over the Technology

- Segregation of responsibilities

  Make contact with the relevant authorities.

  Engagement with subject-matter-specific interest groups about the protection of sensitive information in project management. Examining the procedures for the protection of sensitive information. Review the policies for information securities.

Policies:

The policy on safeguarding human resources encompasses the following areas:

- Pre-employment procedures
  - Evaluation of job candidates
  - Job Requirements and Other Conditions
  - Job description terms and conditions communicated clearly.
  - Penalties for breaching employment contracts

- During job duties

- Responsibilities of supervisors
- Examination of security protocols and obligations
- Introduction to the company's security practices for new hires
- Continuous education, training and awareness about information security
- Inquiries into possible policy violations and privacy violation.
- Obligations upon dismissal from employment.

- The policy includes the following provisions for physical and environmental safety:
  - Establishing a secure physical perimeter
  - Implementing controls for entry to physical areas
  - Safeguarding workplaces, meeting spaces, and storage areas
  - Assuring safety from the elements and other potential dangers
  - Following all necessary safety measures when performing tasks in restricted locations
  - Logistics management for loading and unloading

- The following are some of the themes addressed in the Acceptable Usage Policy:
  - General use and ownership of company resources
  - Protection of security and confidential information
  - Prohibitions on unacceptable use of company resources
  - Specifications for the Use of Systems and Networks
  - Email and other forms of electronic communication guidelines
  - Rules for Media Platforms and Blogging

- The Password Policy contains the following provisions:
  - General password guidelines
  - Recommendations for password selection
  - Protocols for password protection
  - Guidelines for storing passwords securely.

Policy for Clear Desk:

- Guidelines for Device Registration and Protection:
  - Registration of Endpoints and Removal of Registration
  - Generic Security Requirements for Fixed and Mobile Computing Devices
  - Additional safeguards for endpoints that store secret information

- Policy for Managing Logs and Controlling Access to Networked Resources:
  - Requirements for individuals acting as system owners and IT custodians.
  - Password criteria to be met for security purposes.
  - Login requirements that must be satisfied.
  - Log management guidelines for proper record-keeping and monitoring.
  - Guidelines for remote access to the system.

- Deleted Files and Other Electronic Waste Disposal Policy:
  - Delete Information that is neither private nor secret.
  - Keep private information secure.
  - On the other hand, the Technology Equipment Disposal Policy focuses on two aspects:
  - Proper disposal of technology equipment.
  - Guidelines for employees who may wish to purchase disposed equipment.

- The Internet Usage Policy covers several areas, including:
  - Guidelines on the internet services that are permitted to be used.
  - The permissible use of the internet.
  - The use of the internet for personal reasons.
  - The usage that is prohibited.
  - Analysis of data available to the public.
  - Secrecy in email and other forms of electronic communication is expected.
  - Keeping the company's reputation intact through accurate portrayal and utilization of official documents is crucial.

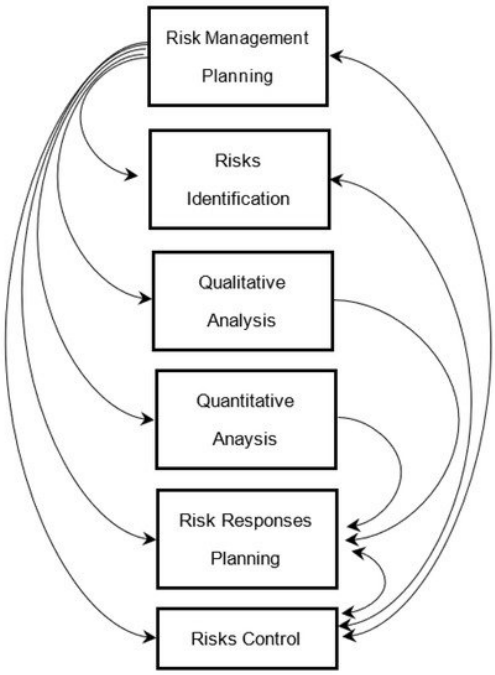
- The need for periodic reviews, including compliance reviews of usage and maintenance reviews of the policy.

- The policy for Internet Use Monitoring and Filtering outlines several measures, which include:
  - Monitoring of website usage.
  - Guidelines for accessing website monitoring reports.
  - Implementation of an internet use filtering system.
  - Guidelines for making changes to internet use filtering rules.
  - Guidelines for exceptions to the internet use filtering policy.

5.3 Handling of the Risks Associated with Information Security:

This policy has been established to guarantee that Amco operates at an appropriate level of risk and to protect the privacy, security, and accessibility of the company's information resources. Whether they are administered in-house or by a third party, all of Amco's information resources fall under the purview of Information Security Risk Management. Executive managers, systems engineers, stakeholders, and IT administrators must work with the appropriate Information Security Office to carry out the information risk mitigation Program. It means fixing newly-identified threats as soon as possible. Classification of risks associated with information resources:

The policy for classifying hazards related to information resources applies universally to all types of information resources, including those used for data storage, analysis, and transfer. Based on the Data Classification Policy, information resources are classified based on their respective functions, susceptibility, and level of risk exposure. This classification approach considers a variety of characteristics, including the size and complexity of information resources, technological infrastructure, the complexity of adopting protective measures, and the potential and significance of threats, particularly those involving sensitive or secret data. (Risk managment & ISMS, 2016).



- Security control selection:

To address known risks, security controls are chosen based on their characteristics, practicality, and cost-effectiveness. Amco has opted to include components from two security control frameworks - ISO 27002 and ITIL - in its approach for managing risks to information security. ISO 27002 offers methods for ensuring network safety and best practices for information security management, whereas ITIL provides common methods and rules for managing IT services. These selected elements will be incorporated into the Amco Information Security Risk Management framework.

The Amco Registration of Endpoints and Removal of Registration policy and the Policy for Protecting Servers at Amco both set out the minimum standards that systems and endpoints must meet to be considered compliant. The controls will be evaluated according to the framework outlined above and implemented based on the risk analysis.

- Risk Analysis:

A documented risk analysis method is used to identify, define, and prioritize risks based on the confidentiality, integrity, and availability of information resources. There are a number of stages to a thorough risk assessment. including but not limited to ranking risks and vulnerabilities to information resources, pinpointing prospective threats that might exploit vulnerabilities, assessing the severity of an individual vulnerability's effect on resource security, and outlining actions and controls to keep resources safe. Whenever there are new security threats, events, or shifts in security needs or infrastructure that might compromise the privacy, reliability, or authenticity of information resources, the risk analysis approach is revised.

In the event that the security measures taken for an information resource do not live up to a certain security standard, risks are recognised and evaluated based on the following three factors: the possibility of the prospective risk occuring as well as the nature of the threat, the efficiency or vulnerability of the existing security mechanisms, and the likely degree of the consequence. The degree of danger posed by an event can be described as high, medium, or low. In the context of this policy, "high-risk scenarios" refer to situations in which there is an immediate danger of sensitive data being compromised or lost from either internal or external sources in the absence of effective protective measures. In a scenario with a medium risk, there is a probability that sensitive data will be compromised or lost, but in a scenario with a low risk, there is a minimal risk that sensitive data would be compromised or lost.

- Risk mitigation

It is very necessary to choose and put into action suitable risk management procedures in order to protect the availability, confidentiality, and integrity of data resources. These safeguards were adopted in order to manage risks in a continuous manner; nonetheless, it is vital to review them on

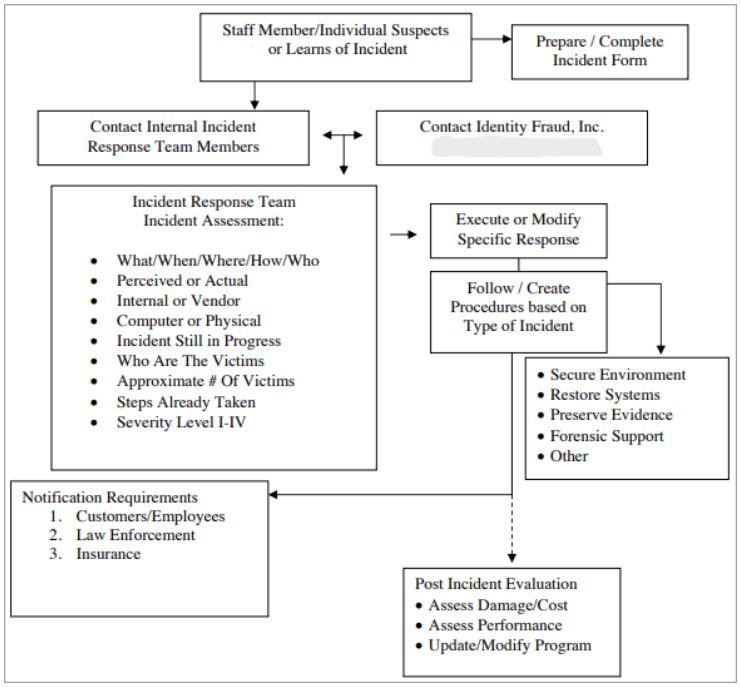
a regular basis and bring them up to date in light of any new facts that may emerge. In the case that an actual incident does take place, the risk evaluation and administration are performed with the new information. Also, the level of urgency and sensitivity of the measures is increased in accordance with the type and extent of the occurrence. In general, risk mitigation is an essential component of information security, and the knowledge and skills I gained throughout my internship helped me appreciate how important it is to the process of safeguarding precious data resources.

- Risk Monitoring

The outcomes of assessing and fixing risks are recorded and assessed by high-level managers, the relevant information security manager, those who own the systems and data, and IT custodians. Compliance with laws, regulations, industry standards, and company policies, as well as the effectiveness of security measures, may all be evaluated with the use of various monitoring techniques. Variables such as the number of interconnected systems, the potential for harm from those connections, the importance or sensitivity of the information resource, and the needs of information security regulations all affect how often risks should be observed. In general, my experience with risk monitoring has taught me the significance of regular monitoring processes to mitigate potential risks and assure compliance with the organization's policies and regulations.

5.4 System for Responding to Data Breaches:

The aim of this policy is to establish a process for responding to security breaches and to clarify its scope, criteria, and metrics. This policy defines a breach, assigns duties, establishes criteria for prioritising incidents, and specifies procedures for reporting them, fixing the problem, and receiving feedback. Amco is dedicated to preventing harm to its workers, clients, partners, and the business as a whole, whether such harm is intended or not.



This policy applies to anybody who is responsible for the management of private or sensitive information, including those who collect, access, process, protect, keep, use, transmit, dispose of, or otherwise handle such information. The same level of responsibility as outlined in this policy shall apply to any agreements with third-party suppliers or business partners.

Reporting of incidents is critical to detecting and mitigating IT security breaches. Any abnormal system behavior or errors may indicate a breach and must be reported immediately by all employees to the InfoSec Team. After determining the gravity of the situation, the InfoSec Team will notify the CEO. The following are examples of IT security incidents that require immediate reporting to the InfoSec Team:

- Stealing actual pieces of information technology hardware, such as computers and storage devices.
- Accessing protected information and then stealing that information in violation of confidentially.
- Observing unusual system behaviour, which may point to the presence of a virus or other form of harmful activity.
- Mistakes made by humans that compromise information technology security or violate IT standards, such as keeping passwords on a computer that is accessible to several users.
- Attempting to access data or systems without being authorised to do so.
- Infecting computer systems with software that is either prohibited or hazardous to use.
- Causing damage to data without authorisation and/or causing damage to data.
- Causing damage to the physical components of information technology equipment like computers and storage devices.
- Making inappropriate use of company information, services, or assets in a manner that breaches established guidelines.
- Making unauthorised alterations to the organization's hardware, software, or configuration, whether intentionally or accidentally.
- Taking action in response to alarms that signal possible breakdowns in security.

According to this policy, anybody who has reason to believe that Amco's confidential or sensitive data may have been compromised or exposed is obligated to promptly send a description of the occurrence through email, the phone, or the reporting website. These channels are monitored by the Information Security Team, which also conducts investigations into any occurrences that are reported in order to determine whether or not a security breach or exposure has taken place. If the allegations are shown to be true, the Information Security Team will respond in accordance with the protocols designed to handle incidents of this nature.

5.5 Confirmed violation:

On confirmation of theft, data breach, or disclosure of Amco's sensitive or private data, access to the affected resource will be suspended. The Executive Director will be notified of the event, and IT and a selected forensic team will begin an investigation to discover the underlying cause. In order to deal with the security breach or potential risk, an incident response team will be assembled, and it will operate under the guidance of the Executive Director. The team responsible for addressing the compromised system or data breach should consist of members from various departments, including Infrastructure, Finance, Legal, HR, and the affected business unit. Additionally, the affected business unit should also be part of the team. With the support of specialists, the team will analyze how the breach or exposure happened, the categories of data involved, the number of persons and organizations affected, and the underlying reason of the breach. Priority will be placed on recovering the lost data. The team will identify which data has been lost, who has been affected, the scope of their impact, and any immediate measures that may be taken to prevent additional harm. In addition, the team will seek to discover the source of the incident, any possible leaks, and devise a way to repair the issue, as well as install additional procedures to prevent a recurrence of the disaster.

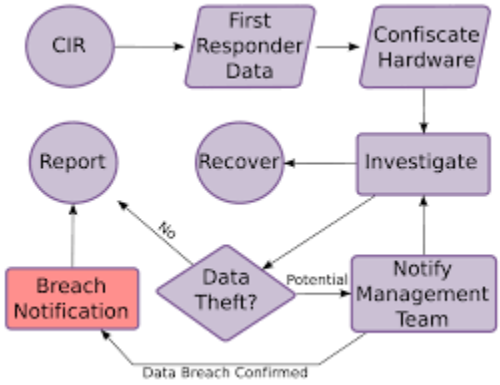


Fig: Overview of workflow (Information Security Incident & Breach Handling Procedure, n.d.)

Chapter 06: Findings of the Study

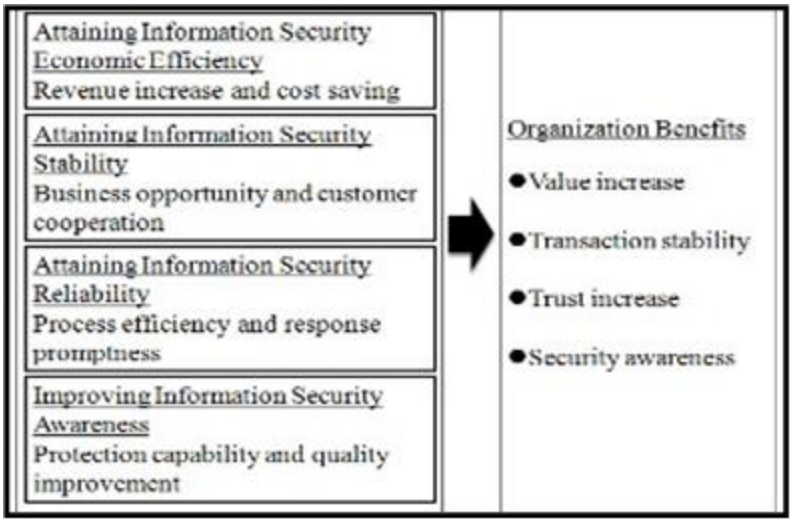
6.1 Advantages of Embracing ISMS Awareness:

Over the course of my study, I came across a number of ideas that I think are relevant to this work and ought to be included. In the first place, increasing ISMS education inside a

company may have a number of benefits, the most important of which is the huge value that can be produced following the successful deployment of ISMS and the achievement of ISO 27001 certification:

- It is possible to quantitatively forecast and keep an eye on the prospective losses that might result from potential risks to the operations of the present information system. Administrators and users alike may get an understanding of the risk levels and take steps to reduce the likelihood that these risks will materialise.
- It is possible to improve the organization's resources in terms of their consistency, productivity, efficiency, and dependability.
- Administrators and users alike can benefit from a heightened awareness of security risks thanks to risk analysis and assessment, which allows for a portrayal of such risks.
- It makes it easier to decide where to put security measures, how to prioritize them, and how much they should cost.
- The public's faith in and the company's ability to compete in today's market can both benefit from government accreditation.
- The company may improve its reputation by assuring customers and suppliers that it abides by relevant regulations, policies, and standards.
- It is possible to fulfill the organization's long-term goals.

Yet, despite the obvious benefits that were stated above, it is possible that such benefits will not be immediately apparent to businesses who receive the certification. As a result, utilizing traditional cost-effectiveness assessments to support the certification of an information security



management system can be dangerous, and it can be difficult to monitor and manage the both tangible and intangible measures that may be further obtained. “ (The Benefits of Implementing an ISMS (Information Security Management System), 2022)”.

The following figure will clarify the points mentioned above

Now, the primary focus of this analysis is to understand how Amco Enterprise Limited benefits from ISMS awareness, particularly as it relates to my organization. Although Amco has not yet obtained ISO 27001 certification, the organization is already experiencing positive impacts. I have recognized many major benefits based on conversations I've had with my direct supervisor, department manager, and IT supervisor, as well as on my personal observations and those of my coworkers:

- Amco security has significantly improved, making the data stored within the organization and on its server much more secure.
- Recent policy changes and additions have increased Amco’s reliability to current clients and potential new clients.
- While maintenance costs have risen, risks have been mitigated, and the organization now has appropriate remedies and actions in place for potential incidents such as data breaches.
- As a result of Amco's adoption of ISMS awareness, the firm has differentiated itself from its rivals and created an extra incentive for clients on a worldwide and local scale to outsource the company with their business operations.
- Amco has expanded its workforce significantly just from five months ago. This growth can be attributed not only to strong performance for clients but also to the recent adoption of ISMS awareness. With policy changes and additions, Amco is attracting more clients than ever before, leading to a larger workforce.

Gradually, Amco is moving closer to achieving its goals. Eventually, it may surpass these objectives and aim for even greater heights. ISMS awareness has been instrumental in the

company's successful journey, and once Amco obtains ISO 27001 certification, it's on track to become a major player in the outsourcing market in Bangladesh and beyond.

6.2 Advantages of Obtaining an ISO 27001 Certification

The Information Security Management System (ISMS) standards are defined in the sole worldwide standard that can be audited, and that standard is ISO 27001. (ISMS). A business that has obtained this certification is able to assert that it utilizes the most up-to-date and effective information security processes.

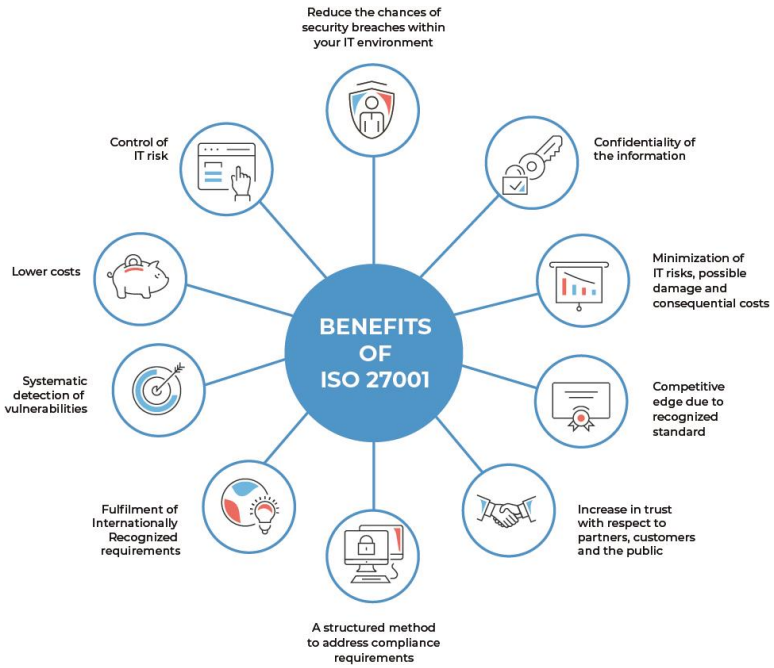


Fig: BENEFITS OF ISO 27001 CERTIFICATION (ISO 27001 – MANAGING INFORMATION SECURITY, n.d.)

The following is a list of advantages that come with obtaining an ISO 27001 certification:

- A company that has this certificate has already been verified on a global scale, so it may immediately gain clients without doing any more verification. This helps an organization get new business and sharpen its competitive edge. Also, clients are likely to place greater importance on a business that possesses this accreditation as compared to similar businesses that do not.
- • Avoid the costs of fines and lost business that might result from a data breach. An rise of 6.4% from the 2017 survey shows that the average cost of a data breach across the globe

is now $3.86 million, as reported by the research organization Ponemon. ISO 27001 accreditation is the international benchmark for effective information asset management, and it may help businesses avoid devastating revenue damage due to data breaches. This is according to the international standard. (Smartlockr, 2022).

- Safeguard and improve reputation in light of the increasing frequency of cyberattacks in today's world. The scenario is especially dangerous for businesses that keep sensitive information on their servers. Hence, if an ISMS that is certified to ISO 27001 is adopted, then the company continues to be secure, and it also demonstrates that the business has taken essential safety, which is a good signal as it assists in the recruitment of customers.
- The purpose of ISO 27001 certification is to ensure that organizations adhere to business, legal, contractual, and regulatory requirements by selecting appropriate security measures that are proportional to the level of risk involved in protecting information. This becomes increasingly important as regulations such as the EU's General Data Protection Regulation and Directive for the Protection of Network and Information Systems from the European Union become stricter. (Baskerville, 2017).
- Adaptation of Structure and Focus: This standard allows firms to be more productive since it clearly sets out the duties for managing the risks associated with information security. This is significant because successful organizations expand quickly, and it does not take very long until there is misunderstanding regarding the allocation of responsibility on information assets.

- After an organization has obtained the certification, it receives an evidence of its effectiveness in terms of security management that is universally recognized, which results in a reduction in the frequency of audits. As a result, the company won't be required to submit itself to audits on a regular basis.

The achievement of ISO 27001 accreditation is a resounding statement that an organization is well protected. Nonetheless, despite this, the organization continues to undergo audits throughout time in order to better itself because there is always opportunity for development. In addition, the auditors make sure to keep a close check on the company to ensure that it does not lose its

concentration on ISMS throughout the course of time. When a business consistently receives favorable reviews following the audits that are carried out at regular intervals that organization progressively develops a positive image of itself, which is really a circumstance in which both the firm and its customers come out on top.

However, what truly matters in the long term is the return on investment. It is important to determine whether the company is seeing the expected increased returns from the expenditures. Incorporating ISMS into the organization's policies is an investment that can reduce costs. For instance, IBM commissioned the Ponemon Institute to research global data breaches. The institute's "Cost of a Data Breach Study" released in 2018 revealed that the average cost of a data breach worldwide was $3.86 million. When compared to the 2017 report, this represents growth of 6.4%. Lost businesses, reputational damage, and staff time spent restoring data are the three most costly outcomes of a data breach. (Smartlockr, 2022).

These things are counted as expenses because they have a direct effect on the finances of the organizations that are impacted by them. Instituting an ISMS policy throughout the organization is an effective means of cost-saving and can promote financial growth for the enterprise. By reducing the cost of data breaches, a company's profitability can increase, and more consumers and businesses may be willing to transact with them. This can result in positive metrics such as return on investment and employee retention.

Having said that, I have worked at Amco for a considerable amount of time and have witnessed significant positive changes during that period. The company's current size is the result of implementing ISMS throughout the organization and pursuing ISO 27001 certification.

Chapter 07: Recommendation & Conclusion

The audit required to obtain the ISO 27001 accreditation has not yet been performed on Amco Enterprise Limited. The management believes that we still have certain things that need to be improved. I had a conversation with my management in order to find out the reasons why the firm

is constantly falling behind its competitors. He discussed a couple of his thoughts. Therefore, based on those observations as well as my opinion, I am going to make some suggestions for areas in which Amco Enterprise Limited could improve in order to pass the audit that is scheduled to take place very soon. This is done in the hopes that Amco Enterprise Limited will be awarded certification.

• Make the working area more compatible to the processing of sensitive data In light of the fact that Amco's office is quite open, it is extremely challenging to uphold the organization's policy of secrecy among its staff members. Amco, however, must prioritize this issue in order to ensure the privacy of its customers' data and speed up the process by which it will be awarded ISO 27001.

• Maintain logs: Amco maintains logs and tracking of organization-owned devices, but it was not deemed essential until recently when the organization became aware of the ISO 27001 certification requirements. It is now crucial to improve the logging and tracking of devices and their users to ensure compliance with the certification standards.

• Strengthen the security measures within the facility: In a place of business such as Amco, it is exceedingly difficult but not impossible to increase the efficiency of the in-house monitoring system that is already in place. They ought to increase the number of security cameras and personnel monitoring the premises.

In conclusion, Amco Enterprise Ltd has to focus their efforts on improving the aforementioned aspects. In the event that this does not change, the effort that has been done over the last several months would have been for nothing, both in terms of acquiring the ISO 27001 certification and developing an efficient ISMS.

Chapter 08: Appendix:

7.1 References

Amco Enterprise Limited company profile. (n.d.). Retrieved from https://amcoenterprise.com: https://amcoenterprise.com/company-profile/

"Ashenden, D. (2008). Information Security management: A human challenge? *ScienceDirect*."

"Baskerville, S. (2017). *Information Security Strategy - 3 Benefits and 3 Implementation Tips*. Retrieved from proserveit: http://www.proserveit.com/information-security-strategy/"

"Boehmer, W. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. *IEEE*."

"Guide to Identifying Personally Identifiable Information (PII). (n.d.). Retrieved from University of Pittsburgh, Information Technology: https://www.technology.pitt.edu/help-desk/how-to-documents/guide-identifying-personally-identifiable-information-pii"

"Heru Susanto, M. N. (2011). Information Security management: A human challenge? *ResearchGate*."

"Information Security Incident & Breach Handling Procedure. (n.d.). Retrieved from https://www.alaska.edu/oit/policies-standards/information-security/"

"Islam, M. Z. (2019, Janurary). *BPO showing great promise*. Retrieved from https://www.thedailystar.net: https://www.thedailystar.net/business/news/bpo-showing-great-promise-1690048"

ISO 27001 – MANAGING INFORMATION SECURITY. (n.d.). Retrieved from https://mooreclear.com/services/iso-27001/

ISO/IEC 27001 Information Security Management System. (n.d.). Retrieved from https://ccqm.ch/certification-process/iso-iec-27001-information-security-management-system/

Mistra, K. G. (2019, November). *Information Security - awareness of Information Security Management System*. Retrieved from Linkedin: https://www.linkedin.com/pulse/information-security-awareness-management-system-misra

Risk managment & ISMS. (2016). Retrieved from enisa.europa: https://www.enisa.europa.eu/topics/threat-risk-management/risk- management/current-risk/risk-management-inventory/rm-isms

Smartlockr. (2022). *The cost of a data breach? On average, $4.4 million per organization*. Retrieved from https://www.smartlockr.io: https://www.smartlockr.io/en/blog/cost-of-a-data-breach

Takieldeen, A. (2019). The Performance of Coding Transmitter Channels to Modern Digital Communication Systems. *ResearchGate*.

The Benefits of Implementing an ISMS (Information Security Management System). (2022). Retrieved from itgovernance: https://www.itgovernance.co.uk/isms-benefits

7.2 Questionnaires:

1. Have you received any training or education on information security management systems (ISMS) or categorization of data in your current organization?
2. How aware are you of the importance of ISMS and data categorization in protecting sensitive data and preventing security breaches?
3. How do you categorize data in your organization, and what factors do you consider when doing so?
4. Are there any specific policies or procedures in place in your organization to ensure the security of different categories of data?
5. Have you encountered any security breaches or incidents related to data in your organization? If so, how were they handled?
6. How often are security risk assessments or audits conducted in your organization, and are the results of these assessments used to improve the ISMS?
7. Do you feel that your organization's current security measures are sufficient to protect against potential security threats? If not, what changes would you recommend?
8. What steps can individuals take to enhance their own awareness of information security best practices and contribute to a culture of security within their organization?
9. Have you ever received any training or education on data privacy regulations such as GDPR, CCPA, or HIPAA?
10. How does your organization ensure compliance with data privacy regulations, and what role do ISMS and data categorization play in this process?

7.3 Progress Report

بسم الله الرحمن الرحيم

AMCO ENTERPRISE LIMITED

امكو انتر برايز ليميتد

وافق وكيل التوظيف الحكومة، رقم الرخصة لر ال ١٥٣٧

Govt. Approved Recruiting Agent License No. RL-1537

Ref: Date:

INTERN MONTHLY PROGRESS REPORT
INTERNSHIP PROGRAM
Fall/Spring/Summer (Fall 2022)
School of Business and Economics
United international University

Student Name: Imam Hossain Shanto		Institutional Supervisor: MOHAMMD ANAMUL HAQUE	
Student ID #:	111182112	Institution Name	AMCO Enterprise LTD.
Major:	Management Information System	Academic Supervisor:	Ahmed Imran Kabir

Activities undertaken during the month

Date 27/12/ 2022	Dept.: Info. Analysis	Activity: I focused on understanding the department's objectives, processes, and data sources.
Date 25/02/ 2023	Dept.: Info. Analysis	Activity: I continued to work on the customer satisfaction analysis project as well as other projects, including analyzing sales data to identify trends and patterns, and creating data models to forecast sales and revenue.
Date 29/03/ 2023	Dept.: Info. Analysis	Activity: I focused on presenting my findings to the department and other stakeholders. I created presentations and reports summarizing the results of my analyses and provided recommendations for improvements.
Date	Dept.:	Activity:
Date	Dept.:	Activity:

Institutional Supervisor's

Date: 29/03/2023 Time: 11.30 AM

Additional Comments

AMCO ENTERPRISE LTD.

Supervisor Signature: Mohammad Anamul Haque Managing Director Date: 29/03/2023

Student Signature: Date: 29/03/2023