Stp Ig Program Implementation – Phase I

Student’s Name

University

**Individuals in the IG Project team**

1. The Southern Region manager – The manager responsible for the southern branches in Houston and Florida will provide operational personnel and access to information on employees and customers that will be required from their branches.
2. Western Region Manager – The Western Region Manager will provide information and personnel about their branches in California and San Diego
3. Information Security Specialist – An information security specialist will provide key expertise in the auditing and risk assessment of the information systems in order to identify areas that are prone to attacks and best practices on prevention and containment strategies.
4. IT Security Expert – They will provide the advice, guidance, and expertise on the IT infrastructure. They will review the infrastructure to identify security breaches and possibly vulnerable areas. The system will also need to be structured in a modular manner to allow installation of security privileges and authorization.
5. Senior IT Manager – The senior IT manager will be providing the authorizations to the entire company information technology systems and infrastructure. They will also provide human resource guidance skills that are essential in team management. The senior manager will be tasked with ensuring proper planning, organization, evaluation, and budgetary approvals.
6. Overland Transport Manager – Provide management information on risks, challenges, and audit of the overland transport on the transportation of the goods.
7. Airways Transport Manager – They will provide information and personnel on the Airway transport organization with respect to the risks, challenges, systems being used and future expansion prospects.
8. Senior Records Manager - The senior records manager tasked with strategizing on recordkeeping practices will ensure access to important records. They will provide information on the systems being used, challenges, risks and security breaches vulnerability as well as expansion expectations.
9. In-house Financial Analyst and Risk Manager – The financial manager will provide information of the financial budgets of the company giving the forecasts of the company and help in managing the budget of the project by providing cost analysis and estimates.
10. VP of Human Resources – The human resource vice president will provide team organizational strategies and models for best performance. They will also help in determining benefits and remunerations that will be accorded to other team members.

**Information requirements**

1. Kentucky

 The state of Kentucky requires the business to keep a document retention policy that will ensure the company performs proper tax payments under the Statutes Section on administrative regulation. Employee records (Parker & Nielsen, 2011). The state requires employers to keep records of all unlawful activities an employee for one year from the day the record was created. An employee is also entitled to access to their records upon a written request to view their file in full or part. All discipline cases and reprimands must be recorded by the supervisors and issue a copy of the document to the employee. All cases of data breaches must be notified to respective people who are affected by the attack

1. The state of Texas

 Texas requires business entities to maintain a basic record of information for inspection purposes in printed or electronic form. Payroll records indicating the wages paid to employees and the hourly rate are required to be kept in a period for not less than three years. The employer is also supposed to keep records of an employee for not less than three years from the day they were hired (Parker & Nielsen, 2011). All forms if disabilities should also be recorded under the ADA for at least one year. Any forms of discrimination associated with age should also be recorded for not less than three years from the day of the claim.

1. California

 The state stipulates guidelines requiring strict adherence to record keeping procedures including sale receipts. Records that include employee information used to review their performance and hiring are stipulated as personal records. The personal record includes everything an employee is involved in including their promotions, benefits, disciplinary actions and disability records (Mann & Roberts, 2015). Employers are required to keep a consistent record of all information about an employee in the workplace while at the same time keeping other confidential information separately. Medical information about employees is kept in a different file from the personal record. California laws require employers to keep records of a time when the employees are working for at least four years.

**Information systems risks**

1. Viruses

 A virus is a malicious software code that is created to purposefully attack a computer system and steal information (Laudon & Laudon, 2016). There are normally downloaded via spam emails or from portable disks. Viruses can infiltrate the company information system from outside when employees or unauthorized people gain access to company computers. Viruses have a different effect and can lead to total failure in the information system. A virus can be programmed to create a backdoor and allow hackers to access the system remotely. This risk cannot be transferred

1. Trojan horse

 This is a malicious code that is added into a genuine software with the aim of creating a backdoor to allow hackers to access the system remotely. Trojan horse poses a danger to the company since the may give hackers the opportunity to create user accounts and escalate privileges. This risk can be transferred by contracting with a company to provide software solutions for the business.

1. Worms

 They are unique kind of viruses that replicate themselves and spread from one computer to another in a company. They can be transferred by contracting an information system security company that will be tasked with antivirus system installation and maintenance.

1. Spyware

 Spywares are software programs that are used to monitor an information system remotely. They can be used to access and collect crucial and sensitive information from the company. Spywares can penetrate the information system through downloaded software and trojans. The risk can be transferred by ensuring the company and installing antispam programs and filters.

1. Spam

 Spams are junk emails that are sent randomly in large quantities. A Spams pose a threat to the information system as it may be used to install worms and trojans. These junk emails can be embedded with malicious spyware or rootkits that install themselves when the email is opened.

1. Rootkits

 Rootkits are low-level programs that run in the background and enable remote access via the network. They give hacker access the privileges and allow them to obtain administrative access to the information system resources. Rootkits can be installed by rogue employees who steal crucial information. They can also be embedded into emails after which they install themselves after being opened. Rootkit threats cannot be transferred hence the need to ensure proper access control system are installed in order to prevent an attack (Dhillon, 1997).

1. Denial of Service

 Denial of service is threats where a hacker uses network overload to send huge packets to a server that finally fails to manage the request and breaks down. They are usually done remotely. The risk can be transferred by contracting a security company that will offer firewall services and server redundancy to ensure the resumption of work of the server fails. The denial-of-service attack is usually aimed at rendering a service or an information system resources unavailable to the intended users.

1. Man-in-the-middle

 Man-in-the-middle attacks involve a hacker targeting a network and hijacking the packets while they are being transmuted. The hacker can then steal crucial data, delete or manipulate information. Man-in-the-middle attacks can be prevented by securing the network by encryption.

1. Phishing

 Involves using fake information to impersonate an individual or entity with the aim of stealing crucial data/ For example creating a fake Facebook page with the domains name [**www.facebook.**](http://www.facebook.me) An unsuspecting user will enter their correct details which will be sent to the hacker in a remote location leading to compromise. Phishing uses emails where the hackers send fake emails that look genuine for different purposes such as changing out the password. This risk can be transferred by contesting a company to provide email antispam programs.

1. Social engineering

 Social engineering involves manipulation of company employees in order to offer their confidential data for authorization purposes. One of the common methods is where a hacker engages a company employee and gains access to their computer. The hacker goes ahead to install malicious software such as keyloggers, and trojans. Social engineering cannot be transpired but can be prevented by training the employees and other system users.

**References**

Dhillon, G. (1997). *Managing information system security*. Macmillan International Higher Education.

Laudon, K. C., & Laudon, J. P. (2016). *Management information system*. Pearson Education India.

Mann, R. A., & Roberts, B. S. (2015). *Business law and the regulation of business*. Nelson Education.

Parker, C., & Nielsen, V. L. (2011a). *Explaining compliance: Business responses to regulation*. Edward Elgar Publishing.

Parker, C., & Nielsen, V. L. (2011b). *Explaining compliance: Business responses to regulation*. Edward Elgar Publishing.