**IT Security and Risk Management**

**September 2022 Examination**

**Q1. As a term, people, process, and technology (PPT) refers to the methodology in which the balance of people, process, and technology drives action: People perform a specific type of work for an organization using processes (and often, technology) to streamline and improve these processes. What do you mean by security awareness for people, process, and technology? (10 Marks)**

**Ans 1**

**Introduction**

People, process and technology is a framework that is used by most organizations to improve the day-to-day activities of their employees and tools efficiently. This framework has helped to map the entire value streams of people, processes, and technology. This helps provide full control and visibility into high-performing teams so they can optimize operations and ship faster. This PPT framework is all about how they work together. The process makes this work more efficiently. Organizations can achieve efficiency by balancing people, processes, and technology relationships between them. The technology change also impacts that they should be a change in people and processes to adopt the new tools. If organizations don’t

Buy Complete from our online store

<https://nmimsassignment.com/online-buy-2/>

NMIMS Fully solved assignment available for**session September 2022,**

your**last date is 29th August 2022**.

Lowest price guarantee with quality.

Charges**INR 299 only per assignment.**For more information you can get via mail or Whats app also

Mail id is aapkieducation@gmail.com

Our website [www.aapkieducation.com](http://www.aapkieducation.com/)

After mail, we will reply you instant or maximum

1 hour.

Otherwise you can also contact on our

whatsapp no 8791490301.

Contact no is +91 87-55555-879

**Q2. Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data. Companies often grant access to information and assets to staff even if it is not relevant to that member of staff’s role. Describe access control methodologies and implementation for purpose of security? Give detailed justifications for your recommendations. (10 Marks)**

**Ans 2**

**Introduction**

The ultimate goal of an access control system is to provide a level of security that reduces risk to an organization. These organizationscenter on data from employee onboarding and offboarding to product plans, financial documents, and customer details. Every organization must pay close attention to how they store, access, and protect their assets. Without proper access control, organization leaves their staff and customers vulnerable to cyberattacks, data theft, or breach of privacy and data protection laws.An access control system controls who can view or use any given resource. This can translate to who can access and edit a particular

**Q3. Started in March 2011, Company X is a New Delhi-based custom software solutions provider company. Company deals in developing and customizing software solutions for clients on a project basis and provides technical and business support in an outsourced capability. The main business and service areas of the company include IT consulting, web design and development, mobile applications development, software development, robotics and Internet marketing. The company has an employee base of 50 people, and it caters clients from a wide range of industries including aerospace, automotive, consumer goods, food, metal fabrication, medical, pharmaceutical and solar panel, among others.**

**Key excerpts are presented based on the interview responses from employees across hierarchy in the company.**

**Excerpt 01:**

**if the productivity is lost in our area, then it directly relates to losing our clients, because we have to deliver our projects within scheduled time. And if client loses the trust, he will not give us more business...**

**Excerpt 02:**

**for my organization, there are two assets which are most important; one is the information which we hold and process, the second one, I will say, the technical human resources who do this job... my organization survives on managing information...**

**Excerpt 03:**

**time to time, there is top management support, but not up to the level what is required in our organization, it is lacking..**

**Excerpt 04:**

**comprehensive information security policy is there, but its compliance is another issue…**

**3a. Based on the information presented above what would be the main areas of concern w.r.t IT Security for Company X? Give justification for each of your observations. (5 Marks)**

**Ans 3a**

**Introduction**

Company core business integrity and staff protection are critical, investing in security in companies are important in protecting against cyber-attacks and security threats. Data breaches are time-consuming, expensive, and bad for business. With strong information security, a company reduces its risk of internal and external attacks on information technology systems. They also protect sensitive data, protect systems from cyber-attacks,

**Q3b. What would be the recommendations which you would like to suggest Company X to safe guard them from any potential security threats. (5 Marks)**

**Ans 3b**

**Introduction**

Data breaches and cyberattacks have, unfortunately, become a common issue that businesses of all sizes need to guard against. Knowing how to prevent potential security threats is crucial to running a company’s operations effectively and securely. Information security threats exist both outside and inside your organization. For Company X to protect the security threats,