DCIT 418

ASSIGNMENT 2

Question 1:

Confidentiality, Integrity, and Availability Requirements for an Automated Cash Deposit Machine:

- **Confidentiality:**
  - Example: Protecting the card information and account number provided by the user from being seen or accessed by unauthorized individuals.
  - Importance: High. A breach in confidentiality could result in financial theft and compromise user privacy.

- **Integrity:**
  - Example: Ensuring that the correct amount of cash is deposited into the user's account without any errors or alterations.
  - Importance: High. Any compromise in integrity could lead to incorrect account balances, causing financial errors.

- **Availability**:
  - Example: Ensuring the cash deposit machine is operational and available for users to make deposits at any time.
  - Importance: Moderate to High. While availability is important for convenience, it's not as critical as confidentiality and integrity.

Question 2:

Assessing Impact Levels of Confidentiality, Integrity, and Availability Loss for Different Assets:

- **A student's public blog:**
  - Confidentiality: Low impact. Since the blog is public, there is little need to protect its content.
  - Integrity: Moderate impact. If the blog is tampered with, it could negatively affect the student's reputation.
  - Availability: Low impact. A temporary unavailability wouldn't cause major issues.

- **University examination department managing sensitive exam papers**
  - Confidentiality: High impact. Protecting exam papers is essential to prevent cheating.
  - Integrity: High impact. Any alteration to exam papers could undermine the fairness of the exam process.
  - Availability: Moderate impact. Although exam papers need to be accessible to authorized personnel, continuous availability isn't necessary.

- **Pathological laboratory information system handling patient data:**
  - Confidentiality: High impact. Patient data is highly sensitive and must be kept private to comply with privacy laws.
  - Integrity: High impact. Any alteration of patient data could lead to incorrect diagnoses or treatment plans.
  - Availability: High impact. The system must be available at all times to ensure timely patient care.

- **University student information system:**

Personal and academic data:

- Confidentiality: High impact. Personal and academic details need to be protected to safeguard students' privacy.
- Integrity: High impact. Any data modifications can significantly affect a student's academic progress.
- Availability: Moderate impact. While system availability is important, it can tolerate short periods of downtime.

- **Routine administrative data:**
  - Confidentiality: Low to Moderate impact. Routine data is generally less sensitive.
  - Integrity: Moderate impact. Correct and accurate information is needed for administrative purposes.
  - Availability: Moderate impact. The system should be available for operational efficiency, but temporary outages are not critical.

- **Library management system:**

Student data:

- Confidentiality: Moderate impact. While student data should be kept secure, it's not as sensitive as medical data.
- Integrity: Moderate impact. Any incorrect data could cause administrative inconveniences.
- Availability: Moderate impact. Availability is important for regular library operations.

Book data:

- Confidentiality: Low impact. Information about books doesn't need to be kept confidential.
- Integrity: Moderate impact. Correct book records are necessary for the smooth functioning of the library.
- Availability: Moderate impact. Temporary unavailability is tolerable, but the system should be available for regular use.

Question 3:

Data Protection Act:

The Data Protection Act provides guidelines for how personal data should be handled by organizations. It ensures that personal information is collected and processed lawfully, fairly, and transparently. The act also gives individuals the right to access their data, request corrections, or even demand its deletion if certain conditions are met. In cases where organizations fail to protect personal data, they could face legal penalties, making compliance essential for businesses.

ISO 27001:

ISO 27001 is an international standard designed to help organizations manage and protect their information systems. It offers a systematic approach to managing sensitive company information by implementing an Information Security Management System (ISMS). This standard is particularly valuable for businesses that handle critical data, as it helps to safeguard against unauthorized access, data breaches, and loss of data integrity. Companies that adhere to ISO 27001 can demonstrate to clients and partners that they take data security seriously, boosting their reputation and trustworthiness.

Furthermore, ISO 27001 encourages regular risk assessments, helping organizations identify vulnerabilities and apply the necessary security controls. This proactive approach ensures ongoing improvement and adaptation to new security threats. Certification under ISO 27001 also provides legal protection in the event of a data breach, as it shows that the organization has taken appropriate steps to mitigate risks.

National Institute of Standards and Technology (NIST):

The National Institute of Standards and Technology (NIST) is a U.S. government agency that provides a comprehensive set of cybersecurity frameworks and best practices. NIST is highly regarded for its cybersecurity framework, which includes guidelines on how organizations can assess and manage their cybersecurity risks. It is widely used across various sectors, from healthcare to finance, to help organizations protect critical information and mitigate cyber threats.

One of the key components of the NIST framework is its emphasis on continuous monitoring and improvement, which allows organizations to stay ahead of emerging threats. The framework also promotes a culture of security awareness within organizations by involving employees at all levels in cybersecurity practices. By adhering to NIST guidelines, organizations can enhance their security posture and reduce the likelihood of data breaches or cyber-attacks, ensuring they remain resilient in a constantly evolving digital landscape.