**Question 1**

**Confidentiality requirements:**

* Protecting the user’s account information thus the account number, card number, serial number, etc. This has ***high importance.*** Because when they are accessed, there can be identity theft or even fraud.
* Protecting the machines’ internal software or configuration. This has ***high importance.*** Getting a hold on this data by unauthorized persons can lead to exploitation and unauthorized access to the software.

**Integrity requirements:**

* The software code should not be altered by unauthorized personnel. This could compromise the integrity of the software. ***High importance***
* Ensuring the accuracy and correctness of deposits. This ensures that the deposit is recorded accurately and credited to their accounts. ***High importance.***

**Availability requirements:**

* The machine must work continuously for users to access and deposit any time they want. ***High importance***
* The downtime of the system should not take much time and the system must work consistently. ***High importance.***

**Question 2**

* A student maintaining a blog to post public information.
  + **Confidentiality: Low**

The information displayed on the blog is meant for the public hence, everyone can see it so the level of impact for the loss of confidentiality is low.

* + **Availability: moderate**

The system should be available for the student to post the information, but system downtime will not actually have a great impact on the post. Hence, the moderate impact.

* + **Integrity: High**

The information should be altered by unauthorized personnel so that the information post will be accurate and reliable.

* An examination section of a university that manages sensitive information about exam papers.
  + **Confidentiality: High**

Examination papers contain sensitive information that must not be accessed by unauthorized personnel hence, they must be very confidential. So, the impact rate is very high.

* + **Availability: High**

Exams papers and other resources must be available and ready to be used when needed to ensure a successful and timely conduct of examinations. Not being available will hinder the conduct of examinations and will cause problems.

* + **Integrity: High**

Modifications to exams papers should be done only by authorized personnel to avoid data alteration.

* An information system in a pathological laboratory maintaining the patient’s data.
  + **Confidentiality: High**

The data of a patient is very high and requires a high level of confidentiality.

* + **Availability: High**

The patient’s data must be ready and available on demand.

* + **Integrity: High**

The patient's data must not be altered or modified by unauthorized personnel.

* A student information system used for maintaining student data in a university that contains both personal, academic information and routine administrative information (not privacy related).
* Personal and academic information
  + **Confidentiality: High**

Students' academic and personal information is extremely sensitive, hence stringent confidentiality procedures are needed.

* + **Availability: High**

For academic and administrative procedures, student personal and academic information must be accessible.

* + **Integrity: High**

Accurate record-keeping and decision-making depend on the integrity of students' academic and personal data.

* **Routine administrative information:**
  + **Confidential: Moderate**

Regular administrative data could not be as private as academic and personal data.

* + **Availability: Moderate**

While normal administrative data accessibility is vital, it is not as vital as academic and personal data.

* + **Integrity: Moderate**

Routine administrative data integrity is vital, but not as vital as that of academic and personal information.

* **Information system as a whole:**
  + **Confidentiality: High**
  + **Availability: High**
  + **Integrity: High**
* A university library contains a library management system, which controls the distribution of books among the students of various departments. The library management system contains both the student data and the book data
* **Student data**
  + **Confidentiality: High**

It's possible that private academic and personal information is contained in the student data in the library management system. Hence, must be kept confidential.

* + **Availability: High**

For the management of the library access and books, the data for students must be available always on demand.

* + **Integrity: High**

The integrity of the student data is very necessary and must not be modified without permission or by authorization.

* **Book data**
  + **Confidentiality: Low**

Book data in the library system is not that sensitive because knowing by the public will not cause any severe damage.

* + **Availability: High**

To effectively and efficiently manage the library systems, the book’s data should always be available on demand.

* + **Integrity: High**

Management of the library use the book data in running the library hence, unauthorized access and modification should not be allowed.

* **Information on the whole library system:**
  + **Confidentiality: High**
  + **Availability: High**
  + **Integrity: High**

**Question 3**

**Data Protection Act**

A collection of rules and laws known as the Data Protection Act is intended to safeguard the confidentiality and integrity of personal information. It describes people's rights about the gathering, storing, and use of their personal data by businesses. According to the Act, businesses and governmental organizations must manage personal data carefully, guarantee its correctness, and limit its use to necessary uses. Additionally, it grants people the ability to view their own data and, if needed, request adjustments or deletion. Striking a balance between an organization's need to gather and use data and an individual's right to control their personal information is the aim of the Data Protection Act. To preserve public confidence and stay out of trouble with the law or heavy fines, compliance with the Act is crucial.

**ISO 27001**

An internationally accepted standard for information security management is ISO 27001. It offers businesses a thorough framework for creating, putting into effect, maintaining, and constantly enhancing their information security procedures. The standard protects the confidentiality, integrity, and availability of information assets by including a broad variety of security controls, including administrative, technical, and physical safeguards. Organizations can prove their dedication to information security and skill in risk management by obtaining ISO 27001 accreditation. A qualified auditor conducts a comprehensive assessment as part of the certification process to make sure the organization's security measures satisfy the strict standards criteria. Organizations can increase consumer trust, strengthen overall security posture, and guarantee compliance with pertinent laws and regulations by putting ISO 27001 into practice.

**National Institute of Standard and Technology**

Within the US Department of Commerce lies the National Institute of Standards and Technology (NIST), a non-regulatory government body. Enhancing measurement science, standards, and technology to foster innovation and industrial competitiveness is NIST's main goal. NIST is well-known for its extensive and extensively used cybersecurity frameworks, including the NIST Special Publication 800-series and the NIST Cybersecurity Framework. These frameworks offer organizations best practices and direction on how to manage risk, create and execute efficient security measures, and safeguard their most important assets from online attacks. Since NIST standards and guidelines are frequently cited as benchmarks for laws, rules, and industry best practices, they have a significant impact not only domestically but internationally as well. The agency's work in fields like biometrics, intelligent systems, and encryption advances a variety of technologies and their dependable and safe use.