# CYB 200 Module Three Case Study Template

After reviewing the scenario in the Module Three Case Study Activity Guidelines and Rubric document, fill in the table below by completing the following steps:

1. Specify which Fundamental Security Design Principle applies to the control recommendations by marking the appropriate cells with an *X*.
2. Indicate which security objective (confidentiality, availability, or integrity) applies best to the control recommendations.
3. Explain your choices in one to two sentences with relevant justifications.

| **Control Recommendations** | **Isolation** | **Encapsulation** | **Complete Mediation** | **Minimize Trust Surface (Reluctance to Trust)** | **Trust Relationships** | **Security Objective Alignment (CIA)** | **Explain Your Choices**  **(1–2 sentences)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals. |  |  | X |  |  | I | Complete Mediation will preserve the Integrity of sensitive data untouched. |
| Monitor all traffic leaving the organization to detect any unauthorized use. |  |  | X |  | X | C | Complete Mediation and Trust Relationship allow us to check any data leaking with improve the confidentiality of the user data. |
| Use an automated tool, such as host-based data loss prevention, to enforce access controls to data even when data is copied off a system. |  |  | X |  | X | I | The integrity of the data would be breach if we do not implement Comple Mediation and Trust Relationship. |
| Physically or logically segregated systems should be used to isolate higher-risk software that is required for business operations. | X |  |  |  | X | A | Isolation and Trust Relationship implementation would keep the business availability to operate open. |
| Make sure that only the resources necessary to perform daily business tasks are assigned to the end users performing such tasks. |  | X |  |  | X | A | The end user oversees a daily task which encapsulates the problem and creates a secure connection between the business and the end user. |
| Install application firewalls on critical servers to validate all traffic going in and out of the server. |  |  | X | X |  | C | Is the traffic is not validated by the firewall, there would not be access (Complete Mediation and Minimize Trust Surface) and will keep the confidentiality of the data/server. |
| Require all remote login access and remote workers to authenticate to the network using multifactor authentication. |  |  |  |  |  |  |  |
| Restrict cloud storage access to only the users authorized to have access, and include authentication verification through the use of multi-factor authentication. |  |  |  | X | X | C | Confidentiality would be preserved by Minimize Trust Surface and Trust relationship since user can access to the data if they do not pass the authentication verification, which stop them to have access if they fail. |
| Make sure all data-in-motion is encrypted. |  | X |  |  |  | I | The data is encapsulated so it cannot be used for malicious users while in motion which will preserve the confidentiality of it. |
| Set alerts for the security team when users log into the network after normal business hours, or when users access areas of the network that are unauthorized to them. |  |  | X |  | X | C | The confidentiality of the data would be preserved by implementing check after normal business our and trace a line of the privilege of the users and connection to the data. |

After you have completed the table above, respond to the following short questions:

1. Is it possible to use DataStore and maintain an **isolated environment**? Explain your reasoning.
   1. DataStore is a popular cloud-based data hosting service that your organization has contracted with to store public-facing information. The only way that DataStore provides isolated environments is if create private service cloud which will store data confidentially and maintained isolated from externa users if this is not the case that data would not be preserve isolated.
2. How could the organization have more effectively applied the principle of **minimizing trust surface** with DataStore to protect its confidential data? Explain your reasoning.
   1. DataStore could effectively apply principles of minimizing trust surface by reducing the number of employees who interact or have access to the data, so it will not have problems like the one mentioned before.
3. How can the organization build a more **security-aware culture** from the top down to prevent mistakes before they happen? Explain your reasoning.
   1. Constant training about security issues (pishing, scams, etc.).
   2. Implementing strict policies that will help to protect the company, users, employees, and customers.
   3. Enforce of change password at least every 4 months and the password need to satisfy certain criteria.
   4. Updating the systems constantly.