Group Members:

Sudipta Halder	2021202011
Mainak Dhara	2021201062
Hari Krishnan U M	2021202022

A.15.1 Information security in supplier relationships

(Mainak Dhara(15.1.1,15.1.2) and Hari Krishnan U M’s(15.1.3) part)

Objective: To establish information security requirements for mitigating the risks associated with suppliers' access to the organization's assets. The control's objective is to ensure that suppliers' access to the organization's assets is secured and that the organization's valuable assets are protected from any security threats that may arise from supplier relationships.

Scope:

- The control applies to all IIITH employees who are closely related to the sysadmin,networking department and all the IT related suppliers who provide hardware and software procurement, network and infrastructure management, cloud services, security solutions, application development and support.
- The scope would be to establish and agree upon information security requirements with suppliers who access, process, store, communicate, or provide IT infrastructure components for the institute's information.

Justification:

- **Information Security Measures for Supplier Interactions :**

  IIIT Hyderabad engages with various suppliers who provide IT services and products, facility management services, and other goods and services that are essential for the functioning of the institute. These suppliers may have access to sensitive information assets belonging to IIIT Hyderabad, such as financial data, research data, student and faculty data, and other proprietary information.

  Consequently, it is crucial for the institute to implement this control, which involves verifying that information security requirements are documented and agreed upon with the vendors. Supplier interactions can pose several risks to the institute's information assets, such as data theft, security breaches, and cyber attacks. Developing an information security plan for supplier interactions can aid the institute in managing these risks by ensuring that the suppliers comply with the necessary security protocols and by providing guidance for continuous assessment and monitoring.
- **Enhancing Information Security through Supplier Agreements and Controls:**

  The institute can strengthen the overall security posture of its information assets by developing and agreeing on information security requirements with suppliers. The provider will be aware of the dangers and their obligations in terms of information security, and they will be legally bound to meet these commitments.Adopting supplier security controls can assist promote transparency between IIIT Hyderabad and its vendors. This involves sharing information on risks, vulnerabilities, and security incidents, which can assist both parties in taking proactive security actions.
- **Addressing Security Risks of ICT Products and Services:** It is necessary to implement control A.15.1.3 in IIIT Hyderabad to address the security risks associated with the use of ICT products and services, especially those introduced by third-party suppliers. By mandating appropriate security measures from these suppliers, the institution can better manage these risks. Additionally, compliance with regulatory requirements related to the management of the ICT supply chain can also be ensured through the implementation of this control.

Procedures:

mainak.dhara@students.iiit.ac.in(Mainak Dhara's part)

- **A.15.1.1 (Information security policy for supplier relationships):**
  The procedure to implement A.15.1.1 control in IIIT Hyderabad can be broken down into the following steps:

  - **Identify the suppliers:** The first step is to identify the suppliers who have access to IIIT Hyderabad's assets or provide IT services to the institute. This can include vendors who supply hardware, software, or provide support and maintenance services.

  - **Assess the risks:** Once the suppliers are identified, a risk assessment should be conducted to determine the potential risks associated with their access to the organization's assets. This assessment should consider the confidentiality, integrity, and availability of the information assets.This includes identifying the likelihood and impact of risks such as data breaches, information leaks, system downtime, etc.

  - **Develop information security requirements:** Based on the risk assessment, information security requirements should be developed that address the risks associated with supplier access to the organization's assets. These requirements should be tailored to the specific needs of IIIT Hyderabad and should be consistent with the institute's information security policies and standards.

  - **Agree on requirements with suppliers:** The information security requirements developed should be communicated to the suppliers, and an agreement should be reached with them. The agreement should be documented, and both parties should sign off on it. The agreement should include specific details on the information security requirements and the consequences for non-compliance.

  - **Implement and monitor the agreement:** Once the agreement is in place, it should be implemented and monitored to ensure that the suppliers are complying with the information security requirements. The monitoring process should include regular assessments and audits to ensure that the suppliers are meeting the agreed-upon standards.

- **A.15.1.2 (Addressing security within supplier agreements):**
  We can follow the following steps in order to implement 15.1.2 in IIIT Hyderabad:

  - Establish a list of relevant information security requirements that are necessary to ensure the security of IIIT Hyderabad's information when suppliers access, process, store, or communicate it.
    - Suppliers must comply with IIIT Hyderabad's information security policies and procedures.
    - Suppliers must implement appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of IIIT Hyderabad's information.
    - Suppliers must provide appropriate security training to their employees who have access to IIIT Hyderabad's information.Suppliers must provide appropriate security training to their employees who have access to IIIT Hyderabad's information.

  - Review and verify the list of information security requirements with each supplier.
    - Suppliers must promptly report any security incidents or breaches that may affect IIIT Hyderabad's information.

- Modify the supplier agreements to include the relevant information security requirements.
    - Suppliers must maintain appropriate records of their information security practices and make them available for audit by IIIT Hyderabad.
- Ensure that all supplier agreements are signed and documented.
- Regularly review and update the information security requirements as necessary.
    - This can be done once a year or when some kind of discrepancy is found and issue is raised by some IIITH employee
    - Necessary changes should be made after consulting with Information security committee of IIITH

- **A.15.1.3 (Information and communication technology supply chain):** hari.u@students.iiit.ac.in (Hari Krishnan U M's part)

    - **Identify the ICT supply chain:** The first step is to identify the ICT supply chain of the organization, including hardware, software, and services. **Example:** Identifying the cloud-based email service as part of the ICT supply chain
    - **Assess the risks:** The next step is to assess the risks associated with the ICT supply chain. This can be done by conducting a risk assessment, considering factors such as the criticality of the ICT supply chain components, the potential impact of their failure, and the likelihood of a risk materializing. **Example:** Assessing the risks associated with the email service, such as the confidentiality and availability of the email data
    - **Implement risk treatment measures:** Based on the risk assessment, appropriate risk treatment measures should be implemented to manage the risks associated with the ICT supply chain. **Example:** Implementing risk treatment measures such as including information security requirements in the contract with the third-party service provider and monitoring their compliance through regular audits
    - **Monitor and review:** The final step is to monitor and review the effectiveness of the implemented measures regularly. This can be done through periodic assessments and audits of the ICT supply chain to ensure compliance with the established requirements. **Example:** Reviewing the effectiveness of the implemented measures periodically to ensure continuous risk management of the email service.

sudipta.halder@students.iiit.ac.in (Sudipta Halder's part)

A.15.2 Supplier Device Delivery Management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

Scope:

- The control applies to all suppliers and includes cloud-based services, managed services, and other IT outsourcing services.
- The scope includes defining specific criteria and requirements for suppliers, monitoring and reviewing supplier performance, and maintaining information security and service delivery at an acceptable level in accordance with supplier agreements.

Justification:

- **Risk management:** By monitoring and reviewing supplier service delivery, IIIT Hyderabad can identify potential risks and take corrective actions to mitigate them. This can help the institute to avoid any disruptions in its operations due to supplier non-performance or other issues. This control is particularly important given the increasing focus on data privacy and security regulations, which require organizations to ensure that their suppliers are complying with the same.
- **Cost savings:** Regular monitoring and review of supplier service delivery can help IIIT Hyderabad identify inefficiencies and cost-saving opportunities. By ensuring that suppliers are delivering the expected level of service, the institute can avoid additional costs associated with rework, delays, or disruptions due to supplier non-performance.
- **Continuous Improvement :** Managing changes to IT services is crucial for the uninterrupted functioning of the institution. By implementing the A.15.2.2 control, the institute can effectively manage these changes. Moreover, the institute places significant emphasis on information security and strives for continuous improvement. By implementing the control, the institute can align with its culture and enhance its information security posture.
  The institute has a dedicated Networking team that possesses the necessary expertise and experience to oversee the implementation of this control and work closely with the suppliers to ensure that the changes are controlled and secure.

Procedures:

- **A.15.2.1 (Monitoring and review of supplier services):**

  - **Establish a process for monitoring and reviewing supplier services:**
    Define a procedure for regularly monitoring and reviewing supplier services.
    Document the procedure and communicate it to relevant stakeholders, including suppliers.
    Example: Develop a process for conducting quarterly on-site reviews of critical suppliers and annual remote reviews of non-critical suppliers.
  - **Define criteria and requirements for evaluating supplier services:**
    Establish security and service level requirements that suppliers must meet.
    Define criteria for evaluating supplier compliance with these requirements.
    Example: Require suppliers to adhere to ISO 27001 or NIST Cybersecurity Framework standards and to provide regular reports on their performance against service level agreements.
  - **Assign responsibility for monitoring and reviewing supplier services:**
    Designate a team or individual responsible for conducting supplier reviews.
    Ensure that this person or team has the necessary skills and resources.
    Example: Appoint the Information Security Manager to be responsible for monitoring and reviewing supplier services.
  - **Develop a schedule for conducting regular reviews of supplier services:**
    Define a schedule for conducting regular reviews of supplier services, based on their criticality and risk.
    Ensure that reviews are conducted at appropriate intervals.
    Example: Conduct quarterly on-site reviews of critical suppliers and annual remote reviews of non-critical suppliers, with an option to conduct additional reviews if necessary.

- **A.15.2.2 (Managing changes to supplier services):**

  - **Establish a process for managing changes to supplier services:**
    Define a procedure for managing changes to supplier services, including requirements for change management and communication.

Document the procedure and communicate it to relevant stakeholders, including suppliers.
Example: Develop a process for assessing proposed changes to supplier services, evaluating their impact on information security and service delivery, and obtaining approval before implementation.

- **Review and approve changes to supplier services:**
  Establish a process for reviewing and approving changes to supplier services.
  Ensure that changes are evaluated against predefined criteria and requirements.
  Example: Require suppliers to submit change requests for review and approval by the Information Security Manager or designated team.
- **Manage and track changes to supplier services:**
  Establish a process for tracking changes to supplier services, including documentation of changes and their impact.
  Ensure that changes are communicated to relevant stakeholders and documented for future reference.
  Example: Maintain a log of changes to supplier services, including details of the change, the reason for the change, the impact on information security and service delivery, and the date of implementation.
- **Monitor changes to supplier services:**
  Establish a process for monitoring changes to supplier services, including ongoing review of service performance and compliance.
  Ensure that changes are evaluated for their impact on information security and service delivery.
  Example: Conduct periodic reviews of changes to supplier services, including assessment of their impact on information security and service delivery, and take corrective action as necessary.