Group Members:

Sudipta Halder   2021202011
Mainak Dhara   2021201062
Hari Krishnan U M   2021202022

Control Number	Control	Applicability	Reasoning
A.15.1.1	Information security policy for supplier relationships **Control :** Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Yes	**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.
A.15.1.2	Addressing security within supplier agreements **Control :** All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the organization's information.	Yes	**Enhancing Information Security through Supplier Agreements and Controls:** The measures indicated in 15.1.2 can be applied by the institution by incorporating appropriate information security clauses in agreements with suppliers. 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.
A.15.1.3	Information and communication technology supply chain	Yes	**Addressing Security Risks of ICT Products and Services:** It is necessary to implement control A.15.1.3 in

	Control : Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.		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.
A.15.2.1	Monitoring and review of supplier services **Control :** Organizations shall regularly monitor, review and audit supplier service delivery.	Yes	**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.
A.15.2.2	Managing changes to supplier services **Control :** Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re assessment of risks.	Yes	**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.