Certificate in Digital Economy Tax

Compliance and Reporting Requirements

ARM CPU: A type of processor designed by ARM Holdings that is commonly used in mobile devices and other embedded systems due to its low power consumption and high efficiency.

API: Application Programming Interface - a set of protocols, routines, and tools for building software and applications. It specifies how software components should interact and APIs allow for communication between different systems and applications.

Artificial Intelligence (AI): The simulation of human intelligence processes by machines, especially computer systems. These processes include learning, reasoning, problem-solving, perception, and language understanding.

Blockchain: A decentralized, digital ledger that records transactions across a network of computers. It ensures that the same transaction cannot be altered or duplicated without the consensus of the network, making it secure and tamper-proof.

Byte: A unit of digital information that typically consists of eight bits.

Cloud Computing: The delivery of different services through the Internet, including data storage, servers, databases, networking, and software.

Compliance and Reporting Requirements: The legal and regulatory obligations that businesses must meet when operating in the digital economy. These requirements include reporting digital transactions, maintaining records, and ensuring data privacy and security.

Cybersecurity: The practice of protecting internet-connected systems, including hardware, software, and data, from attack, damage, or unauthorized access.

Data Analytics: The process of examining data sets to draw conclusions about the information they contain. It involves the use of statistical and computational techniques to identify patterns, trends, and relationships in data.

Data Center: A physical facility that houses computer systems and associated components, such as telecommunications and storage systems.

Data Mining: The process of discovering patterns and knowledge from large amounts of data. The data sources can include databases, data warehouses, the internet, and other information repositories.

Data Privacy: The protection of personal data and the rights and freedoms of individuals in relation to the processing of their personal data.

Database: An organized collection of data stored and accessed electronically.

Digital Economy: An economy that is based on digital computing technologies, including the Internet, mobile networks, and enterprise software.

Digital Signature: An electronic form of a signature that can be used to authenticate the identity of the sender and ensure the integrity of a digital message or document.

Digital Transformation: The integration of digital technology into all areas of a business, fundamentally changing how it operates and delivers value to its customers.

E-commerce: The buying and selling of goods and services, or the transmission of funds or data, over an electronic network, primarily the Internet. These business transactions occur either business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business.

Encryption: The process of converting plaintext into ciphertext, which cannot be easily understood by unauthorized users.

EU General Data Protection Regulation (GDPR): A regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

Firewall: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Fraud Detection: The process of detecting and preventing fraudulent activities in digital transactions.

Internet of Things (IoT): The network of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and network connectivity that enable these objects to collect and exchange data.

Machine Learning (ML): A type of artificial intelligence that allows systems to learn and improve from experience without being explicitly programmed.

Malware: Software that is designed to disrupt, damage, or gain unauthorized access to a computer system.

Network Security: The practice of preventing and protecting against unauthorized intrusion into corporate networks.

Phishing: A cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Ransomware: A type of malicious software designed to deny access to a computer system or data until a ransom is paid.

RegTech: The use of technology to enhance regulatory processes. It involves the use of innovative software and algorithms to automate and enhance compliance processes, including risk management, regulatory monitoring, and reporting.

Secure Socket Layer (SSL) Certificate: A digital certificate that authenticates the identity of a website and encrypts information that is sent to the server using Secure Sockets Layer technology.

Server: A computer or system that provides resources, data, services, or programs to other computers and users on a network.

Software as a Service (SaaS): A software delivery model in which software is hosted by a third-party provider and made available to customers over the Internet.

Virtual Private Network (VPN): A secure network that uses a public network, such as the Internet, to connect remote sites or users together.

Virtual Reality (VR): A simulated experience that can be similar to or completely different from the real world. It is created by a computer and presented to the user in such a way that the user suspends belief and accepts it as a real environment.

Web Application: A software application that runs on a web server and is accessed via a web browser.

Web Scraping: The automated extraction of large amounts of data from websites.

Wi-Fi: A wireless networking technology that uses radio waves to provide wireless high-speed internet connections.

XML: Extensible Markup Language - a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is designed to store and transport data.