Professional Certificate in Operational Technology Engineer (United Kingdom)

# Compliance and Regulatory Requirements.

A2P, Application-to-Person messaging, refers to the process of sending messages from an application to a person, typically used in mobile marketing and notifications. This term is related to compliance and regulatory requirements in the context of data protection and privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union.

ACD, Automatic Call Distribution, is a system used in call centers to distribute incoming calls to available agents. In the context of compliance and regulatory requirements, ACD systems must be designed to ensure that calls are handled in accordance with relevant laws and regulations, such as the Telephone Consumer Protection Act (TCPA) in the United States.

ADSL, Asymmetric Digital Subscriber Line, is a type of broadband internet connection that uses traditional copper telephone lines. Compliance and regulatory requirements for ADSL include ensuring that internet service providers (ISPs) comply with data protection and privacy laws, as well as regulations related to network security and cybersecurity.

API, Application Programming Interface, is a set of rules and protocols that allows different software systems to communicate with each other. In the context of compliance and regulatory requirements, APIs must be designed to ensure that data is exchanged securely and in accordance with relevant laws and regulations, such as the Payment Card Industry Data Security Standard (PCI DSS).

APNIC, Asia-Pacific Network Information Centre, is a regional internet registry that manages the distribution of IP addresses and other internet resources in the Asia-Pacific region. Compliance and regulatory requirements for APNIC include ensuring that IP address allocations are made in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

ARP, Address Resolution Protocol, is a protocol used to resolve IP addresses to physical MAC addresses. In the context of compliance and regulatory requirements, ARP is related to network security and cybersecurity regulations, such as those related to denial of service (DoS) attacks.

ASN, Autonomous System Number, is a unique number assigned to an autonomous system, which is a network or group of networks under a single administrative control. Compliance and regulatory requirements for ASN include ensuring that autonomous systems are operated in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

ATM, Asynchronous Transfer Mode, is a protocol used for high speed network transmissions. In the context of compliance and regulatory requirements, ATM is related to network security and cybersecurity

regulations, such as those related to data protection and privacy laws.

BCP, Business Continuity Planning, is the process of creating a plan to ensure that an organization can continue to operate in the event of a disaster or other disruption. Compliance and regulatory requirements for BCP include ensuring that plans are in place to maintain data integrity and security in the event of a disaster or disruption.

BGP, Border Gateway Protocol, is a protocol used for routing traffic between autonomous systems. In the context of compliance and regulatory requirements, BGP is related to network security and cybersecurity regulations, such as those related to denial of service (DoS) attacks.

BYOD, Bring Your Own Device, refers to the practice of allowing employees to use their personal devices for work purposes. Compliance and regulatory requirements for BYOD include ensuring that personal devices are used in accordance with company policies and regulations, such as those related to data protection and security.

CDN, Content Delivery Network, is a network of distributed servers that deliver content to users. Compliance and regulatory requirements for CDN include ensuring that content is delivered in accordance with regional and international regulations, such as those related to copyright and intellectual property laws.

CE, Conformité Européene, is a marking that indicates a product complies with European Union (EU) health, safety, and environmental regulations. Compliance and regulatory requirements for CE include ensuring that products meet the requirements of EU directives and regulations, such as those related to product safety and environmental protection.

CCTV, Closed-Circuit Television, is a system used for surveillance and security purposes. Compliance and regulatory requirements for CCTV include ensuring that systems are used in accordance with data protection and privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union.

CISO, Chief Information Security Officer, is a senior executive responsible for information security within an organization. Compliance and regulatory requirements for CISO include ensuring that information security policies and procedures are in place to protect data and systems from cyber threats.

Cloud Computing, is a model for delivering computing services over the internet. Compliance and regulatory requirements for cloud computing include ensuring that cloud services are provided in accordance with regional and international regulations, such as those related to data protection and security.

COBIT, Control Objectives for Information and Related Technology, is a framework used for information technology (IT) governance and management. Compliance and regulatory requirements for COBIT include

ensuring that IT processes and procedures are in place to support compliance with relevant laws and regulations.

Compliance, refers to the process of ensuring that an organization is in accordance with relevant laws, regulations, and standards. Compliance and regulatory requirements include ensuring that organizations have policies and procedures in place to maintain compliance with relevant laws and regulations.

COPPA, Children's Online Privacy Protection Act, is a law that regulates the collection and use of personal information from children under the age of 13. Compliance and regulatory requirements for COPPA include ensuring that websites and online services comply with the law's requirements for notice, consent, and security.

CPS, Cyber-Physical System, is a system that integrates physical and computational components. Compliance and regulatory requirements for CPS include ensuring that systems are designed and operated in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

CSP, Cloud Service Provider, is a company that offers cloud computing services to customers. Compliance and regulatory requirements for CSP include ensuring that cloud services are provided in accordance with regional and international regulations, such as those related to data protection and security.

CTI, Computer Telephony Integration, is a technology that integrates computer and telephone systems. Compliance and regulatory requirements for CTI include ensuring that systems are used in accordance with data protection and privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union.

CVSS, Common Vulnerability Scoring System, is a framework used for vulnerability assessment and scoring. Compliance and regulatory requirements for CVSS include ensuring that vulnerability assessments are conducted in accordance with industry standards and best practices.

Cybersecurity, refers to the practice of protecting computer systems and networks from cyber threats. Compliance and regulatory requirements for cybersecurity include ensuring that organizations have policies and procedures in place to protect data and systems from cyber threats.

DaaS, Desktop as a Service, is a cloud computing service that provides virtual desktops to users. Compliance and regulatory requirements for DaaS include ensuring that virtual desktops are provided in accordance with regional and international regulations, such as those related to data protection and security.

Data Protection, refers to the process of protecting personal data from unauthorized access, use, or disclosure. Compliance and regulatory requirements for data protection include ensuring that organizations have policies and procedures in place to maintain compliance with relevant laws and regulations, such as

the General Data Protection Regulation (GDPR) in the European Union.

DBMS, Database Management System, is a software system used for managing and storing data. Compliance and regulatory requirements for DBMS include ensuring that database management systems are used in accordance with data protection and security regulations, such as those related to access control and authentication.

DDoS, Distributed Denial of Service, is a type of cyber attack that involves overwhelming a system or network with traffic. Compliance and regulatory requirements for DDoS include ensuring that organizations have policies and procedures in place to protect systems and networks from DDoS attacks.

DHCP, Dynamic Host Configuration Protocol, is a protocol used for assigning IP addresses to devices on a network. Compliance and regulatory requirements for DHCP include ensuring that IP addresses are assigned in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

DLP, Data Loss Prevention, is a system used for preventing the unauthorized transmission of sensitive data. Compliance and regulatory requirements for DLP include ensuring that systems are used in accordance with data protection and security regulations, such as those related to access control and authentication.

DMZ, Demilitarized Zone, is a network segment that separates a public network from an internal network. Compliance and regulatory requirements for DMZ include ensuring that network segments are configured in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

DoS, Denial of Service, is a type of cyber attack that involves overwhelming a system or network with traffic. Compliance and regulatory requirements for DoS include ensuring that organizations have policies and procedures in place to protect systems and networks from DoS attacks.

DRP, Disaster Recovery Plan, is a plan used for recovering from a disaster or other disruption. Compliance and regulatory requirements for DRP include ensuring that plans are in place to maintain data integrity and security in the event of a disaster or disruption.

DSL, Digital Subscriber Line, is a type of broadband internet connection that uses traditional copper telephone lines. Compliance and regulatory requirements for DSL include ensuring that internet service providers (ISPs) comply with data protection and privacy laws, as well as regulations related to network security and cybersecurity.

EDR, Endpoint Detection and Response, is a system used for detecting and responding to cyber threats on endpoint devices. Compliance and regulatory requirements for EDR include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data

protection.

EUDPD, European Union Data Protection Directive, is a directive that regulates the processing of personal data in the European Union. Compliance and regulatory requirements for EUDPD include ensuring that organizations have policies and procedures in place to maintain compliance with the directive's requirements for data protection and security.

FCPA, Foreign Corrupt Practices Act, is a law that regulates the payment of bribes to foreign officials. Compliance and regulatory requirements for FCPA include ensuring that organizations have policies and procedures in place to prevent the payment of bribes and to maintain compliance with the law's requirements.

FIPS, Federal Information Processing Standard, is a standard used for securing federal information systems. Compliance and regulatory requirements for FIPS include ensuring that federal information systems comply with the standard's requirements for security and authentication.

FISMA, Federal Information Security Management Act, is a law that regulates the security of federal information systems. Compliance and regulatory requirements for FISMA include ensuring that federal information systems comply with the law's requirements for security and authentication.

GDPR, General Data Protection Regulation, is a regulation that regulates the processing of personal data in the European Union. Compliance and regulatory requirements for GDPR include ensuring that organizations have policies and procedures in place to maintain compliance with the regulation's requirements for data protection and security.

GLBA, Gramm-Leach-Bliley Act, is a law that regulates the processing of personal financial information. Compliance and regulatory requirements for GLBA include ensuring that organizations have policies and procedures in place to maintain compliance with the law's requirements for data protection and security.

HIPAA, Health Insurance Portability and Accountability Act, is a law that regulates the processing of personal health information. Compliance and regulatory requirements for HIPAA include ensuring that organizations have policies and procedures in place to maintain compliance with the law's requirements for data protection and security.

IAM, Identity and Access Management, is a system used for managing and controlling access to resources. Compliance and regulatory requirements for IAM include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

ICS, Industrial Control System, is a system used for controlling and monitoring industrial processes. Compliance and regulatory requirements for ICS include ensuring that systems are designed and operated in accordance with regional and international regulations, such as those related to cybersecurity and data

protection.

IDPS, Intrusion Detection and Prevention System, is a system used for detecting and preventing cyber threats. Compliance and regulatory requirements for IDPS include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

IETF, Internet Engineering Task Force, is a organization that develops and maintains internet standards. Compliance and regulatory requirements for IETF include ensuring that internet standards are developed and maintained in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

Incident Response, is the process of responding to a cyber attack or other security incident. Compliance and regulatory requirements for incident response include ensuring that organizations have policies and procedures in place to respond to incidents in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

IoT, Internet of Things, is a network of physical devices that are connected to the internet. Compliance and regulatory requirements for IoT include ensuring that devices are designed and operated in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

IP, Internet Protocol, is a protocol used for communicating data over the internet. Compliance and regulatory requirements for IP include ensuring that IP addresses are assigned and used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

ISO 27001, is a standard used for managing and securing information systems. Compliance and regulatory requirements for ISO 27001 include ensuring that organizations have policies and procedures in place to maintain compliance with the standard's requirements for information security and management.

ITIL, Information Technology Infrastructure Library, is a framework used for managing and delivering IT services. Compliance and regulatory requirements for ITIL include ensuring that IT services are delivered in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

MFA, Multi-Factor Authentication, is a system used for authenticating users. Compliance and regulatory requirements for MFA include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

NAC, Network Access Control, is a system used for controlling and managing network access. Compliance and regulatory requirements for NAC include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

NIST, National Institute of Standards and Technology, is a organization that develops and maintains standards for information security and management. Compliance and regulatory requirements for NIST include ensuring that organizations have policies and procedures in place to maintain compliance with NIST standards and guidelines for information security and management.

OAuth, is a protocol used for authorizing access to resources. Compliance and regulatory requirements for OAuth include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

PCI DSS, Payment Card Industry Data Security Standard, is a standard used for securing payment card data. Compliance and regulatory requirements for PCI DSS include ensuring that organizations have policies and procedures in place to maintain compliance with the standard's requirements for data security and protection.

PDP, Personal Data Protection, is a process used for protecting personal data. Compliance and regulatory requirements for PDP include ensuring that organizations have policies and procedures in place to maintain compliance with relevant laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union.

Penetration Testing, is a process used for testing and evaluating the security of a system or network. Compliance and regulatory requirements for penetration testing include ensuring that tests are conducted in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

PKI, Public Key Infrastructure, is a system used for managing and securing public and private keys. Compliance and regulatory requirements for PKI include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

RBAC, Role-Based Access Control, is a system used for controlling and managing access to resources. Compliance and regulatory requirements for RBAC include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

SAML, Security Assertion Markup Language, is a protocol used for authenticating and authorizing users. Compliance and regulatory requirements for SAML include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

SDN, Software-Defined Networking, is a technology used for managing and controlling networks. Compliance and regulatory requirements for SDN include ensuring that networks are designed and operated in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

SIEM, Security Information and Event Management, is a system used for monitoring and analyzing security-related data. Compliance and regulatory requirements for SIEM include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

SOC, Security Operations Center, is a team responsible for monitoring and responding to security incidents. Compliance and regulatory requirements for SOC include ensuring that teams have policies and procedures in place to respond to incidents in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

SSO, Single Sign-On, is a system used for authenticating users. Compliance and regulatory requirements for SSO include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

TACACS+, Terminal Access-Control Access-Control System, is a protocol used for authenticating and authorizing users. Compliance and regulatory requirements for TACACS+ include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

TCP/IP, Transmission Control Protocol/Internet Protocol, is a protocol used for communicating data over the internet. Compliance and regulatory requirements for TCP/IP include ensuring that IP addresses are assigned and used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

TLS, Transport Layer Security, is a protocol used for securing data in transit. Compliance and regulatory requirements for TLS include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

VLAN, Virtual Local Area Network, is a network segment that is isolated from other networks. Compliance and regulatory requirements for VLAN include ensuring that network segments are configured in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

VPN, Virtual Private Network, is a network that is used for securing data in transit. Compliance and regulatory requirements for VPN include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

WAF, Web Application Firewall, is a system used for protecting web applications from cyber threats. Compliance and regulatory requirements for WAF include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

WEP, Wired Equivalent Privacy, is a protocol used for securing wireless networks. Compliance and regulatory requirements for WEP include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

Wi-Fi, is a technology used for wireless networking. Compliance and regulatory requirements for Wi-Fi include ensuring that networks are designed and operated in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

X.509, Is a standard used for managing and securing public and private keys. Compliance and regulatory requirements for X.509 Include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

XML, Extensible Markup Language, is a language used for representing and exchanging data. Compliance and regulatory requirements for XML include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.

Zigbee, is a protocol used for wireless communication. Compliance and regulatory requirements for Zigbee include ensuring that systems are used in accordance with regional and international regulations, such as those related to cybersecurity and data protection.