

Commercial Data Management [L6M7]

Target Audience: For those who are successful in completing the CIPS Level 5 Advanced Diploma in Procurement and Supply; this represents the final level of CIPS qualifications for those working towards MCIPS Chartered Procurement and Supply Professional.

Hours: 60 Hours

Pre-requisite: You will need to have achieved the CIPS Level 4 Diploma in Procurement and Supply.

1.0 Understand the concept of big data in the global

supply chain

1.1 Evaluate the term big data and the historic rise of its importance to the procurement and supply function

- Transit from technical problem to business

opportunity:

- Increasing data volumes
- Scalability crisis
- Data storage capacity increases
- CPU capacity, speed and intelligence
- Falling cost of IT
- The 3Vs
- Volume
- Velocity
- Variety

1.2 Evaluate the need for big data and the diversity of data sources and types

- Require large volumes of highly detailed data
- Use of Business Intelligence (BI) and analytics
- Driving agility and innovation with big data
- Sources of data:
 - Sensors
 - Devices
 - Third parties

- Web applications
- Social media
- Types of data:
 - Real time vs. delayed
 - Unstructured (text and human language) vs. semi structured (XML, RSS feeds etc.)
 - Audio, video, other devices
 - Multi vs. single dimension
 - Streaming data

2.0 Understand data integrity and its impact on

procurement and supply

2.1 Evaluate the requirement for integrity and confidentiality of data

- Data integrity vs. data security
- Legal aspects such as:
 - The UK Data Protection Act
 - General Data Protection Regulation 2016 (GDPR)
 - EU Data Protection Directive
 - Responsible data handling
 - Non-disclosure agreements (NDA)
 - Intellectual property rights (IPR)
 - Information assurance and risk management for individuals and organisations
- Physical integrity vs. logical integrity

2.2 Assess the implications of data disruption on the organisation

- Data-enabled business models
- Data resilience strategies
- Disruption tolerance networks
- System redundancy

2.3 Evaluate international laws and standards which govern data integrity and security

- International laws such as:
 - UK Data Protection Act
 - Data Privacy Day (Council of Europe)
- International standards such as:
 - ISO/PAS 28000:2007 (Supply Chain Standards)
 - ISO/IEC 27001:2013 and ISO/IEC 27002:2013

(Manage and protect information)

- The Trusted Computing Group
- The Payment Card Industry Data Security

Standard

3.0 Understand the impact of cyber security on procurement and supply

3.1 Evaluate the term cyber security and its implications

- Data security vs. data integrity
- Supply Chain Cyber Security (SCCS)
- Drivers for SCCS such as:
 - Cyber-terrorism
 - Malware
 - Data theft and the advanced persistent threat

(APT)

- Illegal access and changes to data
- Vulnerabilities in software applications and networks discovered and exploited by malicious hackers
 - Counterfeit computer hardware
- Typical activities for minimising SCCS risks such as:
 - Buying only from trusted vendors
 - Disconnecting critical machines from outside

networks

- Educating users on the threats and protective measures they can take

3.2 Assess data security technologies and their usage in the supply chain

- Create completely secure system using a combination of software and hardware-based security
- Software solutions:
 - Encrypt data to protect it from theft
 - Hacker could corrupt the data in order to make it unrecoverable, making the system unusable
- Hardware solutions:
 - Can prevent read and write access to data and offer very strong protection against tampering and unauthorised access
 - Protects the operating system image and file system privileges from being tampered
- Use strict and secure system administration policies:
 - Backups
 - Data masking
 - Data erasure