CIMA P3
RISK MANAGEMENT
ERRATA SHEET

Errata and clarification list for materials covering exams from 4 November 2019 to January 2021

While every effort is taken to ensure your BPP materials are free from errors or inconsistencies, inevitably some items slip through the net for which we sincerely apologise. This document is designed to summarise all those areas where errata have occurred and provides the appropriate corrections and clarifications required to help you pass this exam. These will be addressed in the next edition of our materials.

Course Book

Reference	Details of errata/clarification required
Chapter 1 Section 3	Within the list of typical risk categories that CIMA could examine, there are two further categories that are not currently discussed in the Course Book that we believe you should be aware of: • **Contractual inadequacy risk** arising from an inability to meet certain contractual commitments • **Employee malfeasance risk** arising from offences committed by staff that are not fraud
Chapter 2 Activity 5: Three lines	The activity requires four methods of assurance to be allocated to the most appropriate line of defence, but the methods are only stated in the solution. The four methods of assurance are as follows: • Customer satisfaction surveys • Review of aged debt analysis by credit controller • Employment tribunal • Internal audit report on payroll All other information is correct.
Chapter 2 Section 8.2	Risk registers should show the level of risk before any controls are implemented - it is possible that in the exam, CIMA may use the term '**gross risk**' to explain risks that have not yet been managed.
Chapter 3 Section 4.3	When considering different methods of growth via acquisitions and mergers and the risks they present, one of the key controls that should be used is **due diligence**, which includes not only financial assessments of potential targets but also assessments of strategic fit in terms of shared IT systems, human resource policies, supply chain synergies and competition constraints.
Chapter 3 Section 6	It is possible that in the exam, CIMA may use the term '**disruptive innovation**' when discussing disruption - however, they both mean the same thing. One such example of how technology could disrupt existing business practices is called **robotic process automation** (**RPA**) where an IT application can perform error-free processing on a far wider scale than any human could do, freeing up the human to perform more qualitative and judgemental analysis on the data.
Chapter 3 Section 8.4 Chapter 7 Section 3.5	Both of these sections allude to the term '**CSR**' or **corporate social responsibility**, but CSR is not actually defined in the Course Book. For the purposes of your exam, you should know that CSR relates to the responsibility owed by a company to the society in which it operates (ie a responsibility that extends beyond the legal and financial obligations of any company to its shareholders).
Chapter 5 Section 6.7 and Activity 7	The term '**backflush accounting**' is used but is **not examinable** so you can ignore it for the purposes of the exam.

Chapter 6 Section 6.3	The following is a term that CIMA may use in the exam that we believe you should be aware of: • **Data centres** are networks of powerful computer servers that handle large amounts of data for organisations that require significant processing capacity
Chapter 7 Section 4	It is possible that CIMA may require you to know the following terms for your exam: • **Materiality** - the relative importance of an item to a set of financial statements • **Sampling risk** - the risk of only testing a sample, rather than the whole population • **Non-sampling risk** - poor interpretation of test results or using the wrong procedure
Chapters 8, 9 and 10 (various)	As a result of CIMA amending the P3 blueprint for syllabus area D1, the term 'white hat hacker' is no longer recognised and should instead be described as an **ethical hacker**. In the same vein, a 'black hat hacker' is no longer recognised and should instead be described as an **unethical hacker**.
Chapter 8 Section 3.2	The following is a term that CIMA may use in the exam that we believe you should be aware of: • The terms availability, integrity and confidentiality are key cybersecurity objectives and are sometimes referred to as the **AIC** or **CIA triad**
Chapter 8 Section 4.1 and 4.2	There are a few terms that CIMA may use in the exam that we believe you should be aware of: • **Malvertising** is an online advert that contains hidden malware • **Spear phishing** is when a specific individual is targeted instead of an entire population • Other forms of attack that applications may suffer could include **structured query language (SQL) injection** where data can be accessed via a company's website, **cross-site scripting (XSS) attacks** which uses an innocent third party's website and **buffer overflow attacks**, where a system is bombarded with more data than it can handle
Chapter 9 Section 3	There are a few terms that CIMA may use in the exam that we believe you should be aware of: • **Certificates** authenticate messages or transactions: previously known as secure socket layer (SSL) certificates, these are now known as **transport layer security (TLS) certificates**. These can help to protect organisations from '**man in the middle**' (**MitM**) attacks where two organisations communicate with each other, but a third party is intercepting their transmissions without their knowledge in order to gain some advantage.
Chapter 9 Section 4.1	When considering business continuity arrangements, there are a number of options that an organisation could consider which you may need to be able to explain in your exam: • **Hot back up sites** are duplicated versions of the hardware and software currently in use which can be called into action as soon as a disaster occurs - these are very expensive • **Warm back up sites** are like their hot counterparts but will require time to be configured • **Cold back up sites** provide locations for business continuity but require more time than a warm site to get fully operational - these are generally the cheapest options • **Mirror sites** provide a duplicate of a website that can be used either when there is excessive traffic or in response to a disaster - these may be essential but are expensive
Chapter 9 Section 4.2	The following is a term that CIMA may use in the exam that we believe you should be aware of: • **Network configuration management** (**NCM**) is used to organise the way that an entity communicates internally and externally via various forms of software and hardware
Chapter 9 Section 5.2	There are a few terms that CIMA may use in the exam that we believe you should be aware of: • Various **teams** exist to monitor cybersecurity threats, ranging from **insider threat** and **threat intelligence teams** who attempt to intercept internal and external threats respectively, through to **hunt teams** who seek out as yet unidentified breaches and **incident response teams** who deal with the immediate aftermath of any breach and are generally known as either **computer incident response teams** (**CIRTs**) or **computer security incident response teams** (**CSIRTs**) • Other cybersecurity monitoring techniques include **security information and event management** (**SIEM**) that monitors data activity for patterns which could indicate threats

Chapter 10 Section 2.4	In the real life example of the PCI Secure Software Standard, you may find it helpful to know that PCI stands for **Payment Card Industry**.