

BCS Level 3 Award in Cloud Services
Answer Key and Rationale – QAN 603/0218/5

Question	Answer	Explanation / Rationale	Syllabus Sections
1	C	A Virtual Machine consists of a Virtual CPU, an amount of RAM, a Virtual Hard Drive and typically connects to a network.	1.1
2	A	Linking system activity to an actual person is important because if misuse or security issues arise, it's imperative that you can identify a particular person if required to do so.	1.6
3	C	Groups are a mechanism for grouping users and allowing user accounts to inherit the permissions available to a group, allowing for easier management of access to resources.	1.6
4	B	A service should be tested in line with the residual risk and business impact assessment. This determines how critical a service is and you can align testing against the importance of the service to the business.	2.7
5	D	To allow virtual machines to communicate, you'd expect them to do this over an IP Network. To achieve this, you'd add a Virtual Network Adapter.	1.1
6	A	If users' files are stored in a cloud storage service, they can be accessed where ever the user has an Internet connection. This makes it easier to get access to files, compared with traditional corporate office file shares, which can only be accessed in the office or over a VPN.	1.2
7	C	While A, B and D are loose examples of what might be included in a disaster recovery plan, the main purpose of the plan is to cover all the steps that need to be implemented in a disaster scenario.	2.3
8	B	B best describes the three-two-one backup policy. The purpose is to have the best chance of recovery in a varied amount of situations.	2.10
9	A	The most likely task would be restoring systems in a given order. Deciding to invoke disaster recovery would be the decision of the CEO on the CTO/CIOs guidance. Testing restores wouldn't be done at this time and managing communications with vendors is not suitable in this scenario.	2.5
10	A	The only way to really know if a backup has worked, even if the media, configs and options have been tested, is to do an actual restore i.e. it's only possible to know by testing the backups ultimate purpose.	2.2
11	A	The primary purpose of security groups is to control access to key resources through groups having permissions and users being a member of the group with permission.	1.7
12	C	This is a methodology, so is system independent. System restores restore the "system" i.e. the entire operating system	2.11

Question	Answer	Explanation / Rationale	Syllabus Sections
		environment. Data restores are typically specific files and folders which are captured at the time of backup.	
13	D	A tenant in a cloud service is typically a separate account / logical container within an account. Such a container could easily be used for any of the listed examples depending on how a particular organisation splits its data / customers / departments into segments.	1.3
14	B	An Incremental Backup will use less space over a course of backup cycles than other types of backup. It'll also backup quicker and with less resources as each Incremental Backup uses less space. The speed of restoration is slower as you need to apply Incremental Backups one by one to get back to a working state.	2.1
15	A	Option A is simply a data restore (Files and Folders) into an already existing drive. All other options will restore the Operating System / Application state and would be classified as system level recovery operations.	2.9
16	D	The only way to really know if the restore is good is by either inspecting the content of the files (in D) rather than just checking the file names (in C). A and B are not sufficient as the quality of the backup cannot be known.	2.2
17	A	During disaster recovery it is essential to know who is needed to return service to normal and what they are expected to do, this is the Roles and Responsibilities.	2.6
18	B	B - It's more resilient. Worst case, the backup is on the same media, but independently stored. Best case it's on different media i.e. backed up to hard drive, then to tape, meaning a failure of one media type doesn't negate the ability to restore from backup.	2.10
19	B	To identify a user, best practice is to give them a named account. None of the other workarounds are valid in giving someone an account which they can continue to use in a supportable manner.	1.9
20	A	Differential backups copy all changes since the last full backup i.e. you'll only ever have to restore the full backup and latest differential, regardless of how many days have passed since the full backup.	2.1