What type of tenant is a private cloud?
Single tenant

What type of tenant is a public cloud?
Multi-Tenant

Describe a community cloud
People in the same industry sharing the cost of resources making a cloud-based application. For example, a group of lawyers making a legal application.

Describe Infrastructure-as-a-Service (IaaS)
You are provided with servers, desktops, firewall routers, and more. You install the OS, configure and patch them.

Describe Software-as-a-Service (SaaS)
A subscription-based application that you access with a web browser, e.g. Office 365. You can not migrate to it.

Describe Platform-as-a-Service (PaaS)
This is where you lease a machine with a programming application inside to help create applications. An example is Azure.

Describe Security-as-a-Service (SaaS)
This is where you outsource your identify management. An example is OKTA providing SAML tokens.

In the context of a cloud environment, describe elasticity.
This is where you can increase or decrease resources at the drop of a hat

What type of storage does the cloud use?
A SAN – you need a fast connection

What type of authentication does the cloud use?
The cloud is a third party that uses federated services.

What is a CASB?
Cloud Access Security Broker. Sits between the cloud and customer and monitors and enforces policies.

What is the first stage in risk assessment?
Identify or classify the asset. This determines how it is handled or stored.

What is risk mitigation?
Reducing a risk. For example, using anti-virus software.

Describe risk transference
Offloading risk to a third party but retaining ownership of the asset. For example, car insurance.

What is risk avoidance?
Avoiding an activity because the risk is too high.

What is risk acceptance?
A circumstance where the risk is deemed low, so you do not need to mitigate or avoid it

What is a threat?
Someone who may attack you and expose a vulnerability. For example, leaving a cake on a table where a Labrador is the threat.

What is a vulnerability?
A weakness in your system. For example, an unpatched computer.

What is a quantitative risk?
A risk that can be give a numeric value that represents the cost of the risk.

What is a qualitative risk?
A risk that can be given a grading – usually high, medium, or low.

What is a risk register?
A listing that shows all of the company's risks, the owners, and the treatments.

How often should the risk register be updated?
At least annually

What is GitHub an example of?
A file/code repository where developers suggest solutions for vulnerabilities.

What does the MITRE framework provide?
Information on adversary tactics, techniques and procedures (TTP), made freely available to the public .

Describe capture the flag
An activity used to upskill a workforce by tackling exercises one level at a time. Employees move up to different levels as they become more proficient team members.

What are the four parts of the information lifecycle?
Creation - Use - Retention - Disposal

What is CIS?
The Centre for Information Security. It gives best practices for tackling threats and provides tools for hardening your environment.

What is NIST?
The National Institute of Standards and Technology (a federal agency)

What is the purpose of NIST?
It provides a cyber security framework and helps identify, detect, and respond to cybersecurity events.

What is RMF?
The Risk Management Framework produced by NIST.

What is the purpose of RMF?
Management of organizational risks. It helps select appropriate security control to protect the individuals and assets of an organization.

What replaced the RMF?
The Cyber Security Framework (CSF)

What is the purpose of Cyber Security Framework (CSF)
To focus on individuals and the risks they pose

What is the purpose of ISO 27001?
To provide security techniques

What is ISO 27002?
A code of practice

What is the purpose of ISO 27701?
Privacy information management

What is the purpose of ISO 3100?
Managing risks for organizations and management in general. Information can be found on its website: https://www.iso.org/standard/65694.html.

What is SSAE?
An audit for SOC reports. It provides cheap reports for around $15,000.

What is a SOC Report?
A Service Organization Report that is a verifiable auditing report

What is the purpose of a SOC Type 1 report?
To measure security

What is a SOC Type 2 report?
It is a report on internal controls. It should be restricted to within the company.

What is a SOC Type 3 report?
It is a report containing general information. It is less detailed, and can be distributed to the public.

What is a CPA and what is their purpose?
A Code Public Accountant. They provide SOC reports that are verifiable audit reports. They use SOC Type 2/3 reports to prove your company's reputation to potential stakeholders.

What is IP theft?
Stealing intellectual property

What is data minimization?
The term for collecting only the amount of data required for a particular purpose

What is data masking?
Retaining only partial data so that the full data cannot be stolen. For example: A masked credit card number would look like: **** **** **** 2346

What is tokenization?
This refers to data that is held in a vault and replaced by a token. The data is held by a payment card provider that gives you a token which can be traced back to a primary account number.

What is anonymization?
The removal or masking of personal identifiers in data

What is pseudo-anonymization?
This refers to the replacement or modification of data by another data source

What is the purpose of a privacy notice?
To explain the reason why data is collected, and state how long it will be kept, used, and disclosed .

What is the purpose of a web application firewall, and which layer of the OSI does it operate?
It protects a web server and its applications from attack. It operates Layer 7, the application layer.

What is banner grabbing?
Stealing header information and operating system details from a web server. Telnet, nmap, netcat (nc), NMAP, Curl and DMitry are banner grabbing tools.

What is CSRF?
Cross site request forgery. For example, if you were to log into a website and click a malicious link on a web page.

What are the indicators of Cross Site Scripting (XSS)?
HTML tags (e.g. redirect), or JavaScript (.js) code denoted by ,

var char, or var data.

What is session replay?
Stealing a cookie to perform an attack. Could also be called session hijacking.

Why should you not use shared accounts?
So that you can monitor or audit down to an individual level

What is a SIEM System?
Security Information Event Management. Used for real-time monitoring, aggregating, and correlating security events.

What is the outcome when an auditor visits?
A new policy or change management. An auditor will never stop a process, but they will report it.

Describe a Type I hypervisor
A hypervisor is required so that the host can run virtual machines. A Type 1 hypervisor runs without an operating system. Examples are ESX and Hyper V.

Describe a Type II hypervisor
It is installed on top of existing software, e.g. Windows 10. An example is Oracle Virtual Box.

What are the physical machines that hold the virtual machines called?
Hosts

What is another name for a virtual machine?
Guest

What are the main resources that the host needs?
CPU cores, RAM and fast disk space

What are containers in a virtual environment?
Isolated guest machines

What is sandboxing and why would you use it?
Isolating an application for testing or patching, or because it

is dangerous

What is Linux sandboxing called?
Chroot jail

What is a snapshot?
Taking a copy of a virtual machine to enable you to to roll back at a later date.

What is VM Sprawl?
An unmanaged guest on your network. You don't know it’s there. It will not get patched and will therefore become a vulnerability.

Describe system sprawl
This is what happens when a virtual host runs out of resources

What is VM escape?
This refers to an attack where the attacker gains access to a guest and tries to attack the host

What is VDI?
Virtual Desktop Infrastructure. A pool of virtual desktops that roll on and roll off

What is VDE?
Virtual Desktop Experience. Permanent: settings are saved on exit. Non-permanent: settings are rolled back on exit.

What is TOTP?
A time-based one-time password. Expires in 30-60 secs.

What is Federation Services?
Third-party to third-party authentication

What does Federation Services use?
An extended attribute such as an email address or an employee ID. It also uses cookies.

What protocol does Federation Services need to be set up?
SAML – an XML-based authentication

What is Shibboleth?
An open source version of Federation Services.

Which authentication uses tickets?
Kerberos

How does Kerberos affect replay attacks?
It prevents them by using USN and timestamps

What is OAuth?
Open authentication. It uses tokens and allows you to authenticate to an application using another product.

What is OpenID Connect?
OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol, which allows computing clients to verify the identity of an end-user based on the authentication. Example: When you're making a booking on Airbnb, you might have to authenticate yourself using Facebook or your Gmail address.

What is a service account?
An account with higher privileges to run an application. Example: You may create an account called 'Sophos User' that will be used to run your anti-virus software.

What is PAM?
Privileged Access Management (PAM). It refers to systems that securely manage the accounts of users who have elevated permissions to critical, corporate resources. The administrator logs into a domain with users accounts and then inserts their credentials, probably using MFA. They are redirected to a bastion domain that holds the admin accounts. They are then given limited administrative credentials to carry out admin duty.

Why would someone use a CCTV camera without film?
As a deterrent

What is a technical control?
One that mitigates risks. Example: A screen saver or firewall rules.

What is a physical control that controls access to a datacenter?
Mantrap

Give some examples of managerial controls
Writing policies, completing forms, pen testing, security awareness training.

What is a compensating control?
It is a secondary control that replaces a primary control

What are operational controls used for?
They are used for day-to-day activities

What type of controls are the following: motion sensors, CCTV, guards?
Deterrent controls

What type of controls are the following: CCTV, log files?
Detective controls

What type of control is restoring data?
Corrective control

What type of control is disabling an account?
Preventative control. It could also be called containment.

What type of control does IAM use?
Access control

What is SLE?
The cost of losing a single item.

What is ARO?
The number of losses in a year

What is ALE?
ARO x SLE. The total losses in a year.

What is a hot site?
A backup site that is fully manned, in which data is replicated

immediately. It is the most expensive site to run.

What is a cold site?
A backing site that is not manned. It has no equipment or data, though it does have running water and electricity. It is cheaper to run than a hot site.