Definitions I've forgotten on practice tests

- RPO - recovery point objective: identifies the maximum amount of data, measured in time, that may be lost during a recovery effort
- RTO - recovery time objective: the amount of time expected to return an IT service to operation after failure
- MTD - maximum tolerable down time: longest amount of time that an IT service may be unavailable without causing serious damage
- SLA - service level agreement: written contracts that document service expectations
- Device finger printing via web portal - requires user authentication and gather lots of data to uniquely identify devices
- Data owner - responsible for classification of data
- pulverizing - best way to comply remove data so that it doesn't leak
- TACAS+ - cisco proprietary protocol. Improvement of radius
- Most refquent target of account management reviews are highly privileged accounts
- Biometrics
    - type 1 - valid subject not authenticated
    - type 2 - invalid subject is authenticatd
    - type 3/4 - not associated with biometric
- Keys
    - Primary - uniquely identifies a row
    - Foreign - uniquely identifies a row and matches to another table
    - Referential - not a database key
    - fire extinguishers - this makes me so mad that we have to memorize these types
    - A - Fires that involve solid or organic materials, such as wood, plastics, paper, textiles, or coal
    - B - Fires that involve flammable liquids, such as gasoline, petroleum oil, paint, or diesel
    - C - Fires that involve flammable gases, such as propane, butane, or methane
    - D - Fires that involve combustible metals, such as magnesium, lithium, sodium, potassium, titanium, or aluminium
    - E - electrical
    - F - cooking
- Risk indicators - can provide useful information for organizational planning and a deeper understading of how organizations view risk. Do not handle security response.
- FERPA - protects privacy information of students
- Digital Millennium Copyright act - protects IPS from activities of their customers

- Preservation - Ensure that informatoin related to the matter at hand is protected against alteration or deletion
- Multitasking - handles multiple processes on a single processor by switching them using OS
- Multi-programming - requires modifications of underlying applications
- Incident response phases
    - Detection - most important step is to realize that there is a problem. Must have a machine analyzing network, as well as a person to filter false positives.
    - Response - need to determine an appropriate response. analyize all of the material before making a decision
    - Mitigation - contain the incident. act on the situation to reduce damage and to keep the situation in a manageable state
    - Reporting - summary of incident, indicators, related incidents, actions taken, chain of custody, impact assessment, identity, and next steps to be taken. assess obligations under laws, regulations, and procedures on how to communicate to
    - Recovery - trying to get the asset to a known good state
    - Remediation - need to make sure attack or failure is not successful again. patch the issue, and figure out if this could happen again in future
    - Lessons learned - what happened, what did we learn, any mistakes, what was good, can we do better next time, is there a good plan in place to deal with this in the future?
- Authentication and authorization web languages
    - SPML - an OASIS developed markup languaged to provide service, user, and resource prvisioning between organizations
    - SAML - used to exchange user authentication and authorization data
    - XACML - used to describe access controls
    - SOAP - like REST but has security in mind. Outlines how web service information is exchanged. When requesting access, a SOAP body contains a SAML request or response inside of it
    - REST - Representation State Transfer. an approach that uses HTTP protocol to access and manipulate text without keeping track of any data(or state)
    - OAUTH - open standard for authorization(not authentication) to third parties. Like when you authenticate with facebook, you can then authorize it to go off and manage your photos. Facebook could access your photos until you tell it not to anymore
- Primary storage - ram is primary storage. secondary storage is hdds, solid state, and optical drives

  Whoa.. just got 11/24 on a practice test...
- SIEM helps provide automated analysis and monitoring of logs and security events. not syslog.
- Requiring authentication provides accountability be ensuring actions taken can be tracked to a specific user
- PAT - port address translation allows a network to use any IP address set inside without causing a conclict with the public internet
- LT2p navtively supports non-IP protocols. PPTP, L2F, and IPSec are all IP protocols

- Parrallel test - team activates the disaster recovery site for testing but primary site remains untouched
- 3DES can use 2 or 3 keys
- RFC 1918 is range of 10.0.0.0 - 10.255.255.255
- passive monitoring is : network tap or span port. active monitoring relies on sythetic or previously recorded traffic.
- RSA requiresly only two keys for each user... fucking duh. even if you have 10,000,000 people, they each just need a public and private key to be able to talk to everyone. they go and get the other persons public key before sending messages.