CIS-215 Midterm Review Chapters 1 – 5

Because the exam will be taken at home, you are allowed to use your book and notes. Please be aware that you are not allowed to consult your fellow students. You should take the exam on your own, doing your own work. This list is a fair reflection of the information on the test. Please know that the exam is timed, so please do not approach the exam thinking that you will just look everything up as you go. There will not be enough time to do that.

**Mission Statement, Objectives, Guidelines – The MOG**

- **Mission**: Statement of its ongoing purpose and reason for existence.

- **Objectives**: clearly define the results an organization and its managers want to achieve in a specific time frame.

- **Guidelines**: Provide information on how policy can be implemented

- **Goals**: goals specify specific accomplishments that will enable the organization to meet its objectives.

**BIA vs. BCP vs. DRP – and related knowledge.**

**- BIA:** essentially a catalog of all of an organization’s important business processes that includes information about the criticality of each.

**-** **BCP**: Set of activities required to ensure the continuation of critical business processes when a disaster occurs.

**-** **DRP**: Set of activities concerned with the assessment, salvage, repair, and restoration of damaged facilities and assets that support critical business processes.

**Risk assessment and management: quantitative vs. qualitative; mitigating, accepting, transferring, etc.**

**- Risk assessment:** Carried out to discover, describe, analyze, and evaluate risks

- **Quantitative:** Treat criteria and guidance for assessing and evaluating risks as discreet mathematical valuations.

- **Qualitative:** Assessment with a predefined scope of assets or activities. Collects descriptive information, including information that cannot be reduced to measurable values .

- **Risk Management:** The process of minimizing potential losses

- **Mitigating:** Use of countermeasures to reduce the risks initially identified in the risk analysis.

- **Accepting:** Choosing to forego mitigation of risks.

- **Transference:** Use of insurance as a means for mitigating risk.

**SLE, ARO, MTD, ALE, RTO, RPO, RCO, RCapO, etc.**

- **SLE**: Single Loss Expectancy

- **ARO**: Annual Rate of Occurrence

- **MTD**: Maximum Down Time

- **ALE**: Annual Loss Expectancy

- **RTO**: Recovery Time Objective – Maximum period of time a business process or system will be unavailable during disaster

- **RPO**: Recovery Point Objective – Maximum acceptable amount of data loss or work loss for a given process

- **RCO**: Recovery Consistency Objective – A measure of the integrity and consistency of data in an emergency operations system as compared to the original data in production.

-**RCap**: Recovery Capacity Objective – Measure of processing capacity for a business process during a disaster

**How do we store passwords – in what form? What’s the best practice?**

**- Hashed and Salted**

**If an employee is terminated, is waiting up to a month to revoke access acceptable?** NO

**When thinking about the C-I-A triad, which letter is the most supported by a BCP/DRP?** Availability

Clear-text vs Plain-text vs Ciphertext: cleartext is text that is never meant to be encrypted.

Plaintext 🡪 algorithm 🡪 Ciphertext

VPN technologies

File/email encryption tools/programs (PGP, …)

**Ways that a system can fail: open, closed, safe…**

**- Fail Open:** Control fails and permits all access

- **Fail Closed:** Control fails and blocks all access (Also called fail safe).

**Software languages: Control Flow, Structured, Object Oriented, etc.**

**- Control Flow:** Sequential in nature(if-then, go-to to alter sequence)

- **Structured:** Procedural Structure use subroutines or functions. Structured in blocks of code that are bracketed by keywords

- **Object Oriented:** Provided an environment where objects could be easily reused (96-97)

**Software Development Methods:**

https://en.wikipedia.org/wiki/Software\_development\_process

**Software attack approaches.(page 98)**

**Audits – types, what are they/why are they necessary?(pg 58-59)**

**Baselines**

**System Certification – what are the two parts of this?(pg 21) certification and accreditation**

**Applets vs. Agents(pg 90 and 127)**

Laws/Regulations/Regulatory Agencies associated with: Sarbox, HIPAA, HITEC, FERPA, FISMA, GLBA,… and what they relate to, like, HIPAA = healthcare records (pg 117)

Differentiate between

PII(Personally Identifiable information)

PHI(Protected Health Information)

EPHI(Electronic Protected Health Information)

IDS vs. IPS. Anomaly vs. Signature-based – Advantages/Disadvantages of each

- IDS: Intrusion Detection System

- IPS: Intrusion Protection System

- Anomaly:

Policies vs. Procedures vs. Standards vs. Requirements

Change Control

Security Controls: TAP Deterrent, Preventative, Corrective, Detective, etc.(pg 9, 121-123, 126)

Biometrics: FRR, FAR

Least Privilege vs. Separation of Duties vs. Job Rotation….

Cryptography – asymmetric/symmetric algorithms, PKI, hashing/salting, types of ciphers. What security goals does cryptography achieve? (chapter 5)

What are the four basic forms of a cryptographic attack? (chapter 5)

Password attacks

Authentication vs. Authorization

Kernel, Driver, HAL, etc., from the chapter.