CYBR3600 Final – Dr. Hale – Sample Questions

True/False [___/50]

Circle the correct answer. Each question is worth 5pts each.

1. Corrective Security Controls focus on alerting administrators and preventing future attacks.

   True False

…there will be 10 true/false questions

Multiple Choice [___/50]

2. Single Loss Expectancy is:
   A. The expected cost associated with the loss of all assets incurred by a threat being realized.
   B. The expected loss of goods from a single threat.
   C. The frequency of annualized threat loss expectancy.
   D. The expected cost associated with the loss of one asset incurred by a threat being realized.
   E. All of the Above.
   F. None of the Above.

…there will be 10 multiple choice questions

Short Answer [___/150]

Briefly (i.e. within the space provided) answer the questions below. If you think you need extra paper or can't fit your answers in the space provided, you either write REALLY BIG or you need to **be more succinct**.

3. (25pts) The six steps in the NIST SP 800-39 risk management lifecycle are: *select, monitor, authorize, categorize, asesss,* and *implement*. Order them into the risk management lifecycle and briefly annotate your diagram to describe what happens in each phase.

…there will be 6 short answer questions

Problems [___/150]

4. (50pts) Imagine that you are a policy analyst and you are given the following natural language policy:

   CAMPUS BUILDING ACCESS POLICY

   A. Campus buildings are closed to the public (non-faculty or staff) between the hours of 2am-5am Monday through Friday and 12am to 7am Saturday and Sunday.
   B. Faculty and staff may access the building at all hours on all days.
   C. The library computer lab will remain open 24/7, 365 days a year to all members of the public.

   a) (35pts) Represent this policy formally using first-order logic.
   b) (15pts) Identify a single instance of non-compliance, state it in plain English, and represent it formally.

…there will be 3 problems (long problems will be take home)

Answers:

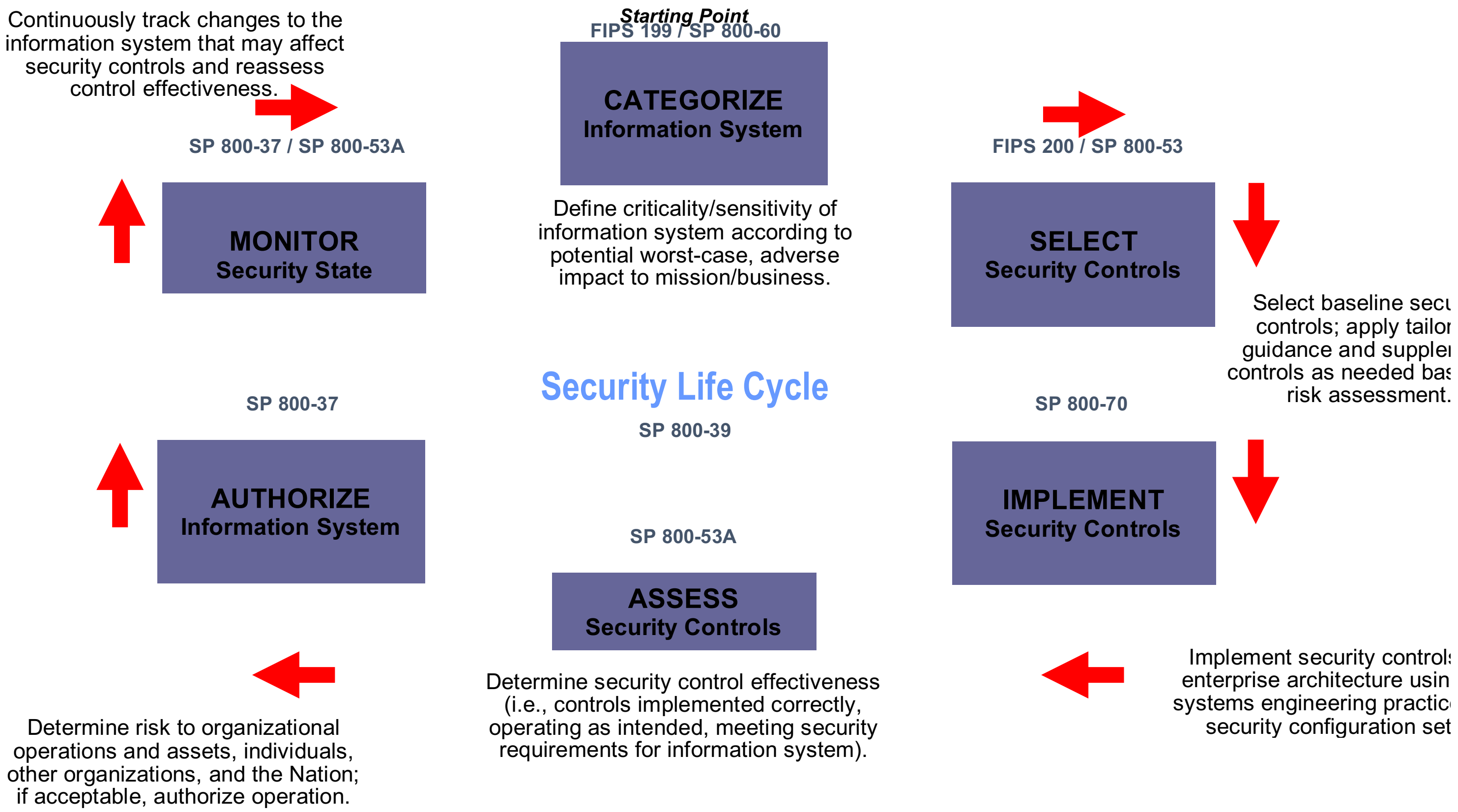
#1

Corrective Security Controls focus on alerting administrators and preventing future attacks.
False – they focus on restoring functionality / service after an attack

#2

D.

#3


Starting Point
FIPS 199 / SP 800-60
CATEGORIZE
Information System
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.
FIPS 200 / SP 800-53
SELECT
Security Controls
Select baseline secu controls; apply tailor guidance and supplei controls as needed bas risk assessment.
SP 800-70
IMPLEMENT
Security Controls
Implement security controls enterprise architecture usin systems engineering practic security configuration set
SP 800-53A
ASSESS
Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).
SP 800-37
AUTHORIZE
Information System
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.
SP 800-37 / SP 800-53A
MONITOR
Security State
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
Security Life Cycle
SP 800-39

#4

Campus building access policy problem:

a) Represent this policy formally using first-order logic.

$\forall b \in \text{Buildings}, p \in \text{Persons}, t \in \text{Time}, d \in \text{Days}:$

$$\begin{aligned}
&\text{Access}(b, p) \Leftrightarrow \\
&\quad (\text{isPublic}(p) \wedge ((d \in \{m, t, w, th, f\} \wedge t \in \{5am \ldots 2am\}) \vee (d \in \{s, su\} \wedge t \in \{7am \ldots 12am\}))) \\
&\vee \text{isFaculty}(p) \\
&\vee b = \text{“library computer lab”}
\end{aligned}$$

b) Identify a single instance of non-compliance.

Many possibilities here, but one might be:
$b \neq \text{“library computer lab”} \land \neg\, \text{isFaculty}(p) \land t = \text{”3am”}$

a building that is not the library computer lab is being used by a non-faculty member at 3 AM