STUDENT HANDOUT · WEEK 16

Final Review, Exam Strategy, and the Project Briefing

SY0-701 objectives 1.0, 2.0, 3.0, 4.0, 5.0. Notes, exercises, review questions, and the lab.

Name	
Date	

THIS WEEK YOU WILL

1. Review the key concepts and common exam traps in each of the five SY0-701 domains.
2. Plan remaining study time in proportion to the domain weights and your own weak spots.
3. Apply a time plan for performance-based and multiple-choice questions on exam day.
4. Use keywords such as BEST, FIRST, and MOST to choose between plausible answers.
5. Translate technical findings into business risk, cost, and decisions for leaders.
6. Prepare and deliver a 10-minute briefing on the Lakeside Family Clinic project.

KEY IDEAS

Study in proportion to the exam weights

12%	1.0 General concepts
22%	2.0 Threats, mitigations
18%	3.0 Security architecture
28%	4.0 Security operations
20%	5.0 Program management
	Domains 4 and 2 are half the exam. On a 90-question exam, 28% is about 25 operations questions.

Domain 1 traps: controls, zero trust, crypto

Trap	Remember
Deterrent vs preventive	Deterrent discourages; preventive actually stops
Hashing vs encryption	Hashing is one-way; encryption is reversible
Signing vs encrypting	Sign: your private key. Encrypt: their public key
Zero trust planes	Control plane decides; data plane enforces
Backout plan	How to undo a change that fails
Salting	Random value so equal passwords hash differently

Domain 2 traps: actors, attacks, indicators

Trap	Remember
Spraying vs brute force	Spraying tries one password on many accounts
Impossible travel	Logins too far apart in too little time
Race condition	TOC/TOU: state changes between check and use
XSS vs request forgery	XSS runs script; forgery sends requests as user
Vishing, smishing	Voice call phishing and SMS text phishing
Unpatchable system	Segment, isolate, and monitor it

Domain 3: design for failure, protect the data

Resilience and design	Data protection
Fail-closed blocks traffic when a device fails	States: at rest, in transit, in use
Inline IPS can block; a tap or monitor only sees	Tokenization swaps data for a token in a vault
Hot site ready now; warm partial; cold space only	Masking hides part of a value, such as ****1234
Load balancing shares load; clustering fails over	Sovereignty: data follows the laws where it lives
Replication copies mistakes too; it is not a backup	Cloud responsibility matrix splits the duties

Domain 4 is the biggest: know these cold

Topic	Remember
SPF, DKIM, DMARC	Allowed senders, a signature, then the policy
SAML vs OAuth	SAML handles sign-in; OAuth delegates access
False positive	Flags something harmless; tune the rule

Topic	Remember
MAC, DAC, RBAC, ABAC	Labels, owner's choice, job role, attributes
IR order	Contain before eradicating; RAM before disk
Sanitize vs destroy	Wipe to reuse; destroy when media is retired

Domain 5: governance, risk, and compliance

Topic	Remember
Policy vs standard	Policy: broad intent. Standard: specific rule
SLE and ALE	SLE = value x EF; ALE = SLE x ARO
Transfer	Insurance moves cost, not accountability
Controller vs processor	Controller decides; processor follows orders
MOU vs MOA	MOU: shared intent. MOA: specific duties
Unknown environment	Testers start with no information

Plan your 90 minutes before you sit down

1. Survey	See whether PBQs open the exam; flag long ones
2. Answer MCQs	Work multiple choice at about a minute each
3. Flag and move	Stuck after a minute? Best guess, flag, go on
4. Return to PBQs	Spend the banked time on flagged simulations
5. Review flags	Change an answer only for a clear reason
6. Answer all	A blank scores zero; never leave one empty

Speak in risk, cost, and decisions

Technical report says	Leadership briefing says
CVSS 9.8 flaw on the VPN appliance	A known flaw lets outsiders into our network
No MFA on remote desktop; 4625 bursts in logs	A stolen password alone opens patient records
Flat network with no segmentation	One infected PC can reach every system we run
Deploy EDR with 24x7 managed monitoring	Tools that spot and stop attacks, about $8,000 a year

EXERCISE 1: ONE SCENARIO FROM EVERY DOMAIN

12 MINUTES · SMALL GROUPS

Answer each scenario, name its domain, and say which word in the question decided your answer.

#	Prompt	Your answer
1	A login banner warns that use is monitored. Control type?	
2	400 accounts, one failed login each, same password. Attack?	
3	A firewall must block all traffic if it fails. Failure mode?	
4	Which log shows who logged on to a Windows server last night?	
5	A vendor offers its SOC 2 Type II report as proof. Audit type?	
6	Asset $40,000, EF 50%, ARO 2. What is the ALE?	
7	The EHR must be back within 4 hours. RTO or RPO?	
8	Which record lists the servers allowed to send a domain's email?	
9	Ransomware is confirmed on one PC. What happens first?	
10	One legacy device cannot be encrypted. What is the response?	

REVIEW QUESTIONS

1. Which two domains together make up half of the SY0-701 exam?

2. To send a confidential message to Dana, which key encrypts it?

3. What is the difference between hot, warm, and cold sites?

4. What should you do when a long PBQ appears at the start of the exam?

5. How should the finding "no MFA on remote access" be stated to clinic leaders?

KEY TAKEAWAYS

- **Study by weight and weakness.** Domains 4 and 2 are half the exam; your weakest domain comes next.
- **Read for the keyword.** BEST, FIRST, and MOST decide between plausible answers.
- **Bank time for PBQs.** Flag long ones, answer the rest, return, and never leave a blank.
- **Brief in business terms.** Lead with the bottom line, the cost, and the decision you need.

LAB 16: FINAL BRIEFING TO LAKESIDE FAMILY CLINIC LEADERSHIP

60 MINUTES

You need your final project report, presentation software, and a timer. The instructor and two classmates act as the clinic's leadership panel: an owner-physician, the practice manager, and the clinic's outside accountant.

Steps

1. Reread your report's executive summary and pick the top three to five risks by score, using the risk register and the ALE figures from your earlier milestones.
2. Write your bottom line in two sentences: the clinic's biggest risk in business terms, and the decision you need from leadership.
3. Build no more than eight slides: the bottom line; how you assessed the clinic; the risk heat map; one slide for each of your top three risks with impact, recommendation, cost, and owner (show any others on the heat map); a 30, 90, and 365-day roadmap; and the decisions requested.
4. Replace every acronym and tool name with a plain description, or define it once in a few words. Move technical detail to the report appendix, not the slides.
5. Prepare answers to five likely questions, including the cost of doing nothing, what the cyber insurance covers, and the cheapest useful step the clinic can take this month.
6. Rehearse twice with a timer. Aim for eight minutes so two remain for questions, and cut content rather than talking faster.
7. Deliver the briefing to the panel. Stand, make eye contact, speak to the decision, and answer questions honestly; if you do not know, say you will follow up.
8. Right after the briefing, write down every question the panel asked and how you would improve each answer.

Hand in

Your slide deck (eight slides or fewer), a one-page leave-behind summary for the panel, and a half-page reflection on the questions you received and what you would change. Submit them with your final project report.

Questions to answer in your report

1. What was your bottom line, and could each panel member restate it after the briefing?
2. Which finding was hardest to translate into business terms, and how did you do it?
3. Which recommendation did the panel push back on, and what trade-off did they raise?
4. If leadership could fund only one recommendation, which would you choose, and why?