

Week 4 workshop: governance and strategic planning

Work in pairs or small groups. Use the slides. Write short answers.

Part A: Governance versus management (10 minutes)

A1. In your own words, what is the difference between governance and management?

A2. Write G (governance) or M (management) for each: (1) The board decides customer data must meet UK GDPR. (2) The IT team sets up encryption on all laptops. (3) The board reviews a quarterly security report and asks questions. (4) A security manager writes the password-change procedure. (5) The board decides how much to invest in security. (6) A manager checks staff finished their training.

A3. ISO 27014 has five governance processes: Evaluate, Direct, Monitor, Communicate, Assure. Write one short meaning for each.

Part B: What do these terms mean? (20 minutes)

B1. TERMS AND ACRONYMS (fill in the three white columns)

Term	Stands for	What is it?	Who is it for?
ISO/IEC 27014 Slides 9 and 10			
GRC Slide 6			
CISO Slides 8 and 11			
EISP Slide 21			
ISSP Slide 22			
SysSP Slide 23			
SMART Slide 30			
MOOC Slide 35			
SETA Slides 33 to 36			

B2. FROM POLICY TO PROCEDURE

B2. Take this topic: reporting phishing emails. Write one line each for the policy, standard, guideline and procedure.

Part C: Small research task (15 minutes)

Choose one: Equifax (2017), Uber (2016 breach, disclosed 2017) or TalkTalk (2015). Use reliable sources such as the ICO website, regulator reports or reputable news.

C1. What happened, and when?

C2. Which of the six ISO 27014 principles was broken? Give one.

C3. Was this a governance failure, a management failure or both? Explain.

C4. Name one governance change that would have helped.

Part D: Start the coursework (15 minutes)

D1. List the governance weaknesses stated in the AeroLink scenario.

D2. Using slide 11, who should own security at AeroLink? Say what each level does.

D3. Which issue-specific policy does AeroLink need most? Why?

D4. Write one SMART objective for AeroLink governance.

Part E: Strategic planning and SETA (20 minutes)

Read slides 28 to 36 first (5 minutes). Then answer in pairs.

E1. A company decides: "We will grow safely online." Write one strategic, one tactical and one operational statement for the security team.

E2. Why can the security team and the IT department disagree? Whose job is each?

E3. SMART stands for Specific, Measurable, Achievable, Relevant, Time-bound. Rewrite this weak goal as a SMART objective: "Improve staff security awareness."

E4. SETA stands for Security Education, Training and Awareness. Write E (education), T (training) or A (awareness) for each: (1) a master's degree in cyber security, (2) a hands-on session on checking a caller before a password reset, (3) a monthly one-minute security tip, (4) a university evening course, (5) a fake phishing email test, (6) a Coursera MOOC on cloud security.

E5. Design a small SETA plan for AeroLink staff and partners: one education, one training and one awareness activity. Add one way to measure whether it works.

Part F: Catch-up on Weeks 1 to 3 (20 minutes)

Choose one scenario and circle it: TechTraders (online shop) | MediCare (health provider) | FinSecure Bank | EduFlex (school) | GovBook (government agency)

F1. Users Who uses or runs the system?

F2. Data types What information does it hold? Which is most sensitive?

F3. Processes What are the main things it does?

F4. Threats Name one internal, one external and one accidental threat. Which tenet does each break (confidentiality, integrity, availability)? What would the consequence be?

F5. Law Which law or standard applies?

F6. Ethics What would be legal but still questionable?

F7. Whole class: law is the minimum and ethics is what you should do. For your scenario, give one thing the law requires and one thing ethics asks beyond that.