

EE2066 Engineers in Society

Test # 1

Time Limit: 30 minutes

Instructions:

1. This test consists of 8 multiple-choice questions. All questions are compulsory and carry equal marks.
2. For each question, select and briefly explain the single best answer.
3. There is no penalty for incorrect answers.

Grading scheme

- **Total Marks:** 80
- **10 marks** each correct answer (highlighted in red). No explanation needed.
- **5 marks** (partial credit) for a plausible incorrect answer (highlighted in green) if the student provides a brief explanation (at least 1-2 sentences) that demonstrates valid thought process or partial understanding of the concept.
- **0 marks** for incorrect answers with no explanation or an explanation that is irrelevant.

Note for students: If your answer deviated from the rubrics but you believe it demonstrates a valid thought process or partial understanding (e.g., a well-explained alternative perspective), please email to schedule a discussion. I am happy to review and consider adjustments for better grades if the reasoning merits it.

Question 1

An engineer at a Hong Kong-based semiconductor company discovers that the company's new chip design has a potential overheating issue that could cause device failures in 2-3% of units under extreme conditions. The marketing department argues that this falls within "acceptable industry standards" and launching on schedule is critical for market competitiveness. According to the multi-lens ethical decision-making framework, what is the **strongest** ethical position for the engineer to advocate for?

- A. Apply the Care Ethics lens to prioritize maintaining relationships with colleagues while documenting concerns through proper channels.
- B. Use the Justice Lens to ensure equitable treatment by following the same risk standards that competitors apply to similar products.

- C. Prioritize the Rights Lens principle that individuals have the right not to be harmed, even if aggregate benefits might favor launch.
- D. Apply Virtue Ethics by considering what a professional engineer of good character would do when balancing competing stakeholder interests.
- E. Resolve the conflict by conducting additional risk assessment to quantify whether utilitarian benefits truly outweigh rights violations.

(5 marks, any one of the following)

- *D shows understanding of professional character in ethical decisions. (However, virtue ethics provides less concrete guidance than rights-based analysis when harm is quantifiable.)*
- *E demonstrates systematic thinking about risk quantification. (However, this delays decision-making when ethical principles already provide clear direction about potential harm.)*

(Why other options get 0 marks)

- *A misses the core ethical priority of preventing harm, focusing instead on relationships, which is secondary here.*
- *B equates "acceptable standards" to competitors and ignores absolute ethical duties (e.g., no harm). It's a weak position without deeper reasoning, as it prioritizes market equity over safety, demonstrating misunderstanding of justice in engineering ethics.*

Question 2

Following a deepfake CEO fraud incident, a Hong Kong fintech company implements multiple countermeasures: multi-channel verification for transactions above HK\$1 million, real-time voice analysis software, mandatory cooling-off periods for urgent requests, and quarterly deepfake awareness training. According to the NIST Cybersecurity Framework, which aspect of their response strategy **best** demonstrates mature implementation of the "Protect" function?

- A. The voice analysis software provides technical safeguards through automated detection capabilities.
- B. The multi-channel verification requirement establishes procedural safeguards that address the attack vector directly.
- C. The quarterly training program builds organizational awareness and human-centered protective capabilities.

- D. The cooling-off periods create temporal safeguards that reduce urgency-based decision-making errors.
- E. The implementation of strict access control policies, ensuring that financial transfers can only be executed from authorized devices and networks, regardless of the request.

[Option B is the best answer. The implementation of multi-channel verification demonstrates the highest level of security maturity because 1) it addresses the fundamental flaw exploited by the attack (trust in a single, compromised channel); 2) it implements a robust, time-tested security principle (out-of-band verification); and 3) it creates a resilient process that is much harder to bypass than a single piece of technology (A), a reliance on human awareness (C), or a control that only addresses a specific tactic like urgency (D).]

(5 mark)

E. However, this was not mentioned as part of their actual implemented measures and appears to describe a hypothetical additional control.

(Why other options get 0 marks)

- *A focuses on a single tech tool, which is less mature than procedural safeguards in NIST's "Protect" function. It ignores the holistic, resilient approach emphasized, showing a narrow view without valid reasoning.*
- *C, while awareness is important, it is more "Identify" than "Protect" in NIST.*
- *D addresses tactics but not the core attack vector (trust in channels). It is a tactical fix, and lacks broader protective strategy insight.*

Question 3

After the IoT system failure, the company implements comprehensive incident response including technical root cause analysis, customer communication, compensation programs, and process improvements. However, they classify the detailed technical findings as proprietary and do not share specifics with industry partners. From an industry-wide cybersecurity resilience perspective, which aspect of their response strategy represents a missed opportunity for collective learning?

- A. The proprietary classification prevents industry-wide vulnerability assessment and collaborative defense development.
- B. The compensation focus may create moral hazard encouraging companies to take excessive risks with customer systems.
- C. The customer communication does not address broader public awareness of IoT security risks for informed consumer choices.
- D. The internal process improvements do not address regulatory gaps that enabled the widespread system dependencies.
- E. The root cause analysis methodology may not be transferable to other companies with different technical architectures.

(5 marks, any one of the following)

- *C understands importance of broader stakeholder education. (However, industry collaboration has more direct impact on collective cybersecurity resilience than general public awareness.)*
- *D recognizes systemic regulatory issues in cybersecurity. (However, this focuses on government action rather than industry self-regulation and knowledge sharing.)*

(Why other options get 0 marks)

- *B speculates on unintended consequences but misses the question's focus on industry-wide learning from the incident.*
- *E critiques internal processes but ignores the key missed opportunity of sharing findings externally.*

Question 4

The renewable energy project involves different engineering standards (IEC vs IEEE), regulatory frameworks (EU directives vs national codes), measurement systems (metric vs imperial), and professional liability concepts. The documentation must serve both design collaboration and legal compliance across jurisdictions. The project's primary constraints are a tight budget that prohibits extensive translation services and a critical need for clear legal defensibility in each country. Which approach **best** balances technical accuracy with cross-cultural accessibility for this complex multinational engineering project?

- A. Create modular documentation with common technical core and jurisdiction-specific appendices addressing local legal and regulatory requirements.
- B. Develop parallel documentation streams optimized for each cultural context with cross-referencing for consistency verification.
- C. Use international standards (ISO/IEC) as the primary framework with conversion tables and equivalency matrices for local variations.
- D. Implement standardized IEEE referencing with consistent terminology while providing comprehensive glossaries for cultural adaptation.
- E. Establish primary documentation in English with professional translation and technical review by native speakers in each jurisdiction.

(5 marks, any one of the following)

- *C shows understanding of international standardization benefits. (However, conversion tables do not fully address legal defensibility requirements in different jurisdictions.)*
- *E recognizes language barrier importance and technical accuracy needs. (However, this approach exceeds budget constraints explicitly mentioned in the scenario.)*

(Why other options get 0 marks)

- *B is inefficient and costly, directly conflicting with the budget constraint. It shows no consideration of practical limitations in multinational projects.*
- *D imposes one standard without addressing legal/jurisdictional needs, missing the balance of accuracy and accessibility*

Question 5

A software development team at a financial services company is under pressure to release a new mobile banking app. During testing, they find a minor data synchronization bug that occurs intermittently. Because previous releases with similar "minor" bugs did not cause major incidents, and the project manager is focused on data showing high overall system stability, the team dismisses the bug as an "acceptable operational anomaly" to meet the deadline. This behavior is an example of:

- A. Correlation-Causation Neglect, as they assume the lack of past incidents means the bug is harmless.

- B. Confirmation Bias, as the team is selectively focusing on stability data that supports their goal of launching, while ignoring the contradictory evidence of the bug.
- C. Selection Bias, as they are only testing the app on the newest phone models where the bug appears less frequently.
- D. Memory Bias, as they can only recall the successful launches and have forgotten the near-misses from previous bugs.
- E. An Echo Chamber, as the entire company culture promotes launching on time above all other metrics.

(5 marks, any one of the following)

- *A identifies logical reasoning error about past incidents. (However, the primary issue is selective attention to favourable data rather than causal reasoning errors.)*
- *D recognizes how past experience influences current decisions. (However, the scenario describes active data selection rather than memory limitations.)*

(Why other options get 0 marks)

- *C: The scenario does not involve biased testing samples (e.g., phone models); it is about ignoring bug data.*
- *E implies groupthink across the company, but the issue is the team's selective focus on data, not a cultural echo. It doesn't fit the decision-making error described.*

Question 6

A major cloud service provider experiences a global outage after an engineer deploys a faulty configuration script to its core network routers. This was not a malicious attack but an internal error. Millions of client services go offline. The post-incident review praises the company for its transparent communication and its ability to restore all services within 3 hours using pre-planned rollback procedures. This incident and its resolution underscore a critical shift in modern cybersecurity strategy, emphasizing:

- A. The need for AI-powered code review to prevent faulty scripts from ever being deployed.
- B. The superiority of human oversight over automated deployment systems.

- C. The importance of robust disaster recovery and resilience capabilities to minimize downtime when prevention inevitably fails.
- D. The critical role of government regulation in mandating specific deployment protocols for critical infrastructure.
- E. The inherent danger of centralizing critical infrastructure with a single cloud provider.

(5 marks, any one of the following)

- *A shows understanding that prevention is important. (However, the scenario emphasizes successful recovery rather than prevention improvements.)*
- *B recognizes human factors in system reliability. (However, this focuses on prevention rather than the resilience approach highlighted in the scenario.)*

(Why other options get 0 marks)

- *D praises internal resilience, not external mandates*
- *E critiques cloud reliance but ignores the resolution's emphasis on resilience, showing misunderstanding of the shift to recovery-focused cybersecurity.*

Question 7

Engineers designing a new building elevator system analyze the predicted failure rates. They estimate a catastrophic brake failure rate of 1 in 10,000,000 trips. They decide to allocate most of their safety budget to addressing more frequent issues, such as door sensor malfunctions (1 in 25,000 trips) and sudden stops due to power fluctuations (1 in 75,000 trips), citing these as more common sources of user complaints. Based on historical engineering disasters and risk assessment principles discussed in class, what is the **most significant flaw** in this reasoning?

- A. The sample size used to calculate the failure rate may be statistically insufficient for reliable predictions.
- B. Building codes (legal safety regulations) usually require elevator brake systems to have backups built in, no matter what the engineers calculate the probability of failure to be.
- C. Low-probability events can have catastrophic consequences that outweigh statistical likelihood.

- D. Elevator brake failures and power outages require fundamentally different analytical frameworks.
- E. Optimal resource allocation should always prioritize highest probability risks.

(5 marks, any one of the following)

- *A demonstrates understanding of statistical reliability concerns. (However, the core issue is risk prioritization methodology rather than data quality.)*
- *B shows awareness of regulatory safety requirements. (However, this does not address the fundamental flaw in the risk assessment approach.)*

(Why other options get 0 marks)

- *D is irrelevant. The flaw is in risk prioritization, not analytical methods for specific failures.*
- *E directly contradicts historical lessons (e.g., black swan events), showing a fundamental misunderstanding of risk assessment in engineering.*

Question 8

A company designs and sells high-end laptops. To assess the long-term reliability of their battery, their engineering team analyzes data only from units that have *not* been returned under warranty after three years of use. They find that these "surviving" laptops show excellent battery health and declare the design a success. The **most significant** ethical failure resulting from this analytical error is:

- A. A lack of Honesty and Integrity, because the marketing team will now use this misleading data to advertise the product.
- B. A failure in the "Get the Facts" stage of ethical decision-making, as the analysis is based on an incomplete dataset.
- C. *A violation of their duty to the public, as they are ignoring the failure data from returned units, which could reveal a critical defect that poses a fire safety risk in all devices.*
- D. A violation of responsibility to colleagues, as it invalidates the efforts of the customer service team who handle the returns.
- E. A failure of transparency, as the full reliability data is not made available to regulatory bodies.

(5 marks, any one of the following)

- **A recognizes marketing implications of misleading data.** (However, focuses on commercial dishonesty rather than public safety, which is the primary ethical concern.)
- **B identifies the fundamental analytical error.** (However, this focuses on methodology rather than the **ethical implications/consequences** of ignoring safety risks.)

(Why other options get 0 marks)

- *D misses the public safety implications.*
- *E is important but not the "most significant" flaw. The core issue is ignoring safety risks, not just reporting.*