[**Homework 14**](https://github.com/hendraanggrian/IIT-ITM511/blob/assets/assignments/hw14.pdf)**: Resilience engineering**

**Problem 1**

*Explain how the complementary strategies of resistance, recognition, recovery, and reinstatement may be used to provide system resilience.*

1. **Resistance:** The system is expected to produce a resisting strategy that adapts to the incoming threat. Critical components of the system are of the utmost importance and should be guarded when under attack.
2. **Recognition:** The ability to detect active threats and predict future problems for better preparation. Acknowledging the existence of a threat is crucial to trigger the resistance.
3. **Recovery:** Prioritize the reactivation of core services when the inevitability of system failure occurs, be it a security attack or hardware failure. Minimizing user interruption is the aim of the recovery strategy.
4. **Reinstatement:** The last stage ensures that all services should be reactivated. The system has proved its resilience.

**Problem 2**

*What are the types of threats that have to be considered in resilience planning? Provide examples of the controls that organizations should put in place to counter those threats.*

1. **Asset confidentiality:** Bad actors may capture unauthorized access to collect data (Sommerville, 2016). To mitigate the risk, patch security vulnerabilities and adhere to standard security practices.
2. **Asset integrity:** The system has been exploited, and data may be manipulated against our benefit or corrupted to disrupt the operation. Organizations often depend on backups and recovery management to reinstate the system.
3. **Asset availability:** The system is uninterrupted but its access is severely limited at the network level by external forces. To protect against such threats, organizations can adjust their bandwidth or ban the IP addresses of violators.

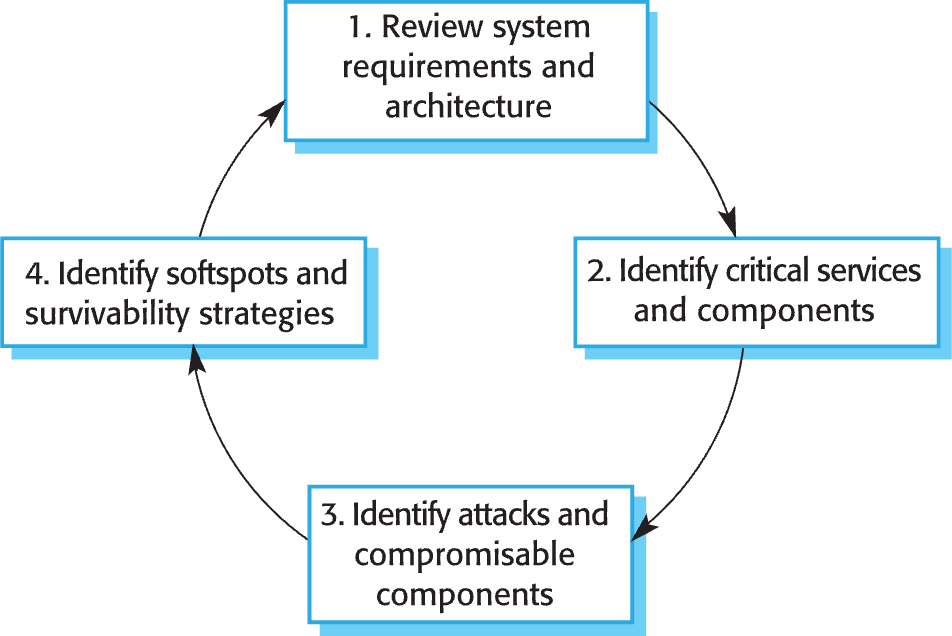
**Problem 3**

*A hospital proposes to introduce a policy that any member of clinical staff (doctors or nurses) who takes or authorizes actions that leads to a patient being injured will be subject to criminal charges. Explain why this is a bad idea, which is unlikely to improve patient safety, and why it is likely to adversely affect the resilience of the organization.*

Doctors and health workers are sworn in to protect the well-being of their patients. Despite that, they are unlikely to perform professional and unbiased work when the outcome may result in self-imprisonment. Moreover, incidents during the patient's treatment are unintentional wrongdoings and do not warrant criminal charges. Resilience planning should rely on active collaboration among participants instead of capital punishment.

**Problem 4**

*What is survivable systems analysis and what are the key activities in each of the four stages involved in it as shown in* ***Figure 14.8****?*

**

***Figure 14.8*** *Stages in survivability analysis*

Analysis of survivable systems is a cycle of four stages that reports the current system's capability in light of recent attacks.

1. **Understand the system:** Gather information about the system's purpose, resources, and other relevant points.
2. **Identify critical service:** Acknowledge certain components with higher priority and isolate them from the rest due to their importance to the users.
3. **Simulate attack:** Anticipate threat by running through every common attack scenario.
4. **Analyze survivability:** Produce a report of the system's resource evaluation and deterrence strategy.

**Problem 5**

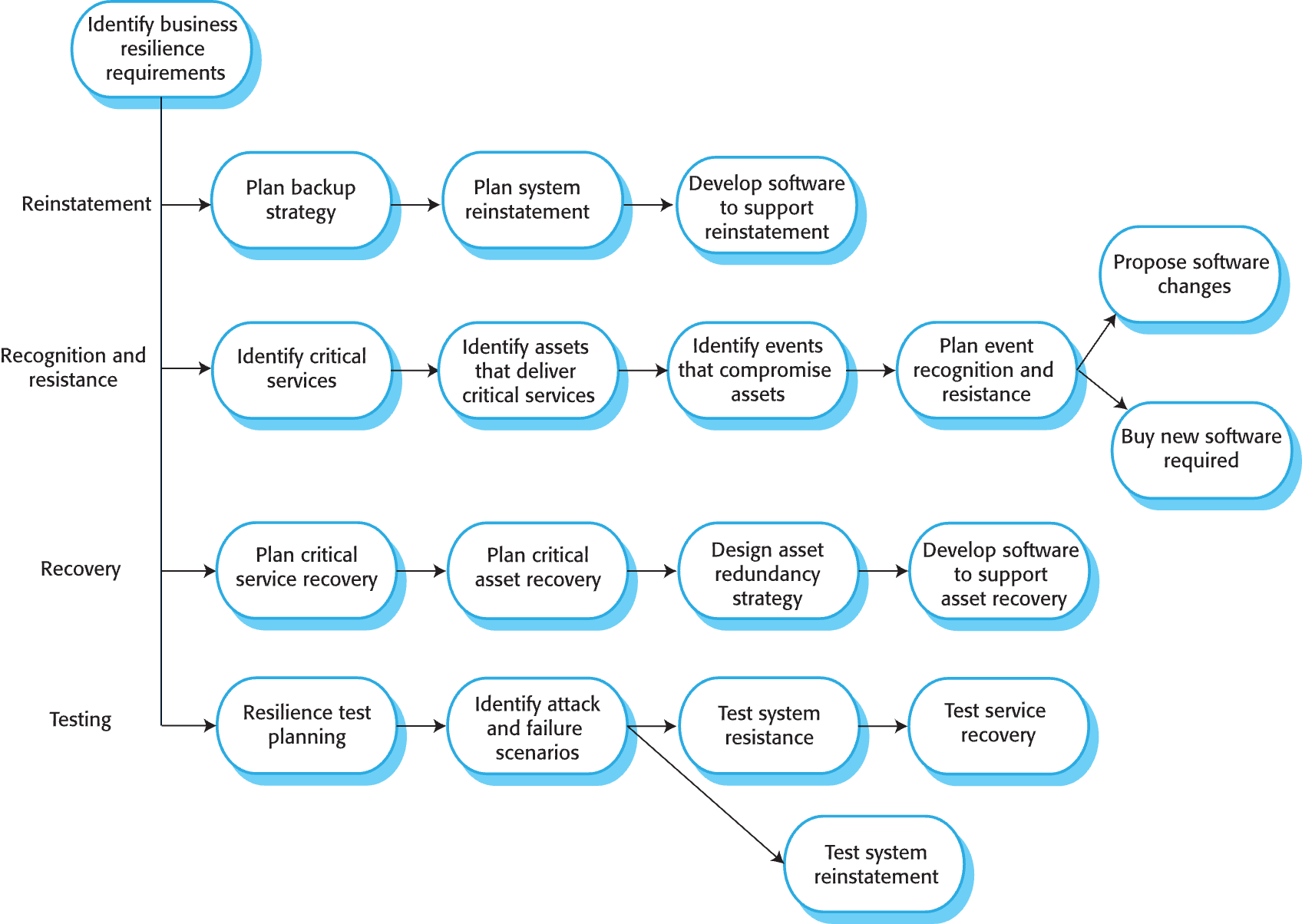
*Explain why process inflexibility can inhibit the ability of a sociotechnical system to resist and recover from adverse events such as cyberattacks and software failure. If you have experience of process inflexibility, illustrate your answer with examples from your experience.*

In an event such as software attacks and internal failure, the system's survivability is inherently connected to sociotechnical relations including the humans operating them. Being inflexible with the circumstances can slow performance, leading to delayed response. The problem is exacerbated when recovery points or other mitigation strategies are unavailable, highlighting the organization's poor planning.

In my limited experience with process inflexibility, a team I was part of voted to uphold the legacy technology, refusing to the modern programming languages and practices in the process. Our resistance to change made us trapped in a less-supported environment and hindered our overall performance.

**Problem 6**

*Suggest how the approach to resilience engineering that is proposed in* ***Figure 14.9*** *could be used in conjunction with an agile development process for the software in the system. What problems might arise in using agile development for systems where resilience is important?*

**

***Figure 14.9*** *Resilience Engineering*

Resilience engineering refers to a five-step process that recovers and tests affected components. Although it can be implemented in an unsupported system, it can also be integrated into an agile software development methodology, taking into account safety restrictions in an iterative approach.

However, the fast movement of agile methodology may conflict with the safety checks, in which the software team would need to balance agility and resilience. Integration with other services can also pose an incompatibility risk if the required resilience is too complex to simulate.

**Problem 7**

*A senior manager in a company is concerned about insider attacks from disaffected staff on the company’s IT assets. As part of a resilience improvement program, she proposes that a logging system and data analysis software be introduced to capture and analyze all employee actions but that employees should not be told about this system. Discuss the ethics of both introducing a logging system and doing so without telling system users.*

* **Log the systems:** Internal activities of an organization should be transparent so that misdeeds can be traced back to the original actor. Nevertheless, there is an ethical debate on how much data is enough when exposing user information to the record logs.
* **Log with no user acknowledgment:** To justify this action, the software team can use a psychological assumption that malicious actors are more likely to commit misdeeds when they are not warned about the impending logs. Even so, using this strategy promotes a culture of suspicion and quite possibly violates regional laws regarding consumer data protection (Tsukayama & José, 2022).

**Problem 8**

*In* ***Section 13.4.2****, (1) an unauthorized user places malicious orders to move prices and (2) an intrusion corrupts the database of transactions that have taken place. For each of these cyberattacks, identify resistance, recognition, and recovery strategies that might be used.*

1. Malicious orders

* **Resistance:** Validate user input so that every submitted order is composed of correct formatting and in-range value. Authenticate the user session before important actions can be taken.
* **Recognition:** Conduct regular check that detects suspicious behavior when an order is submitted. Determine and track activities from suspected entities.
* **Recovery:** Design a fail-safe strategy when an order is under suspicion of threat to avoid impact on market prices. Alternatively, increase the data backup frequency of market prices until the bug is fixed.

1. Corrupted transactions

* **Resistance:** Configure database permission to restrict access to higher-level functionality. Comply with security guidelines such as data encryption and hashing.
* **Recognition:** Identify and monitor accounts related to the corrupted transactions. Study a pattern in how the system can be exploited.
* **Recovery:** Perform a forensic analysis of the attack to get a full picture of security vulnerabilities. Attempt to repair them in the next deliverable of the project.

# **Bibliography**

Sommerville, I. (2016). Software Engineering. In *Cybersecurity* (10 ed., p. 413). Pearson Education.

Tsukayama, H., & José, M. (2022, 12 26). *Privacy Shouldn't Clock Out When You Clock In: 2022 in Review*. Retrieved from Electronic Frontier Foundation: https://www.eff.org/deeplinks/2022/12/privacy-doesnt-stop-when-you-clock-2022-review/