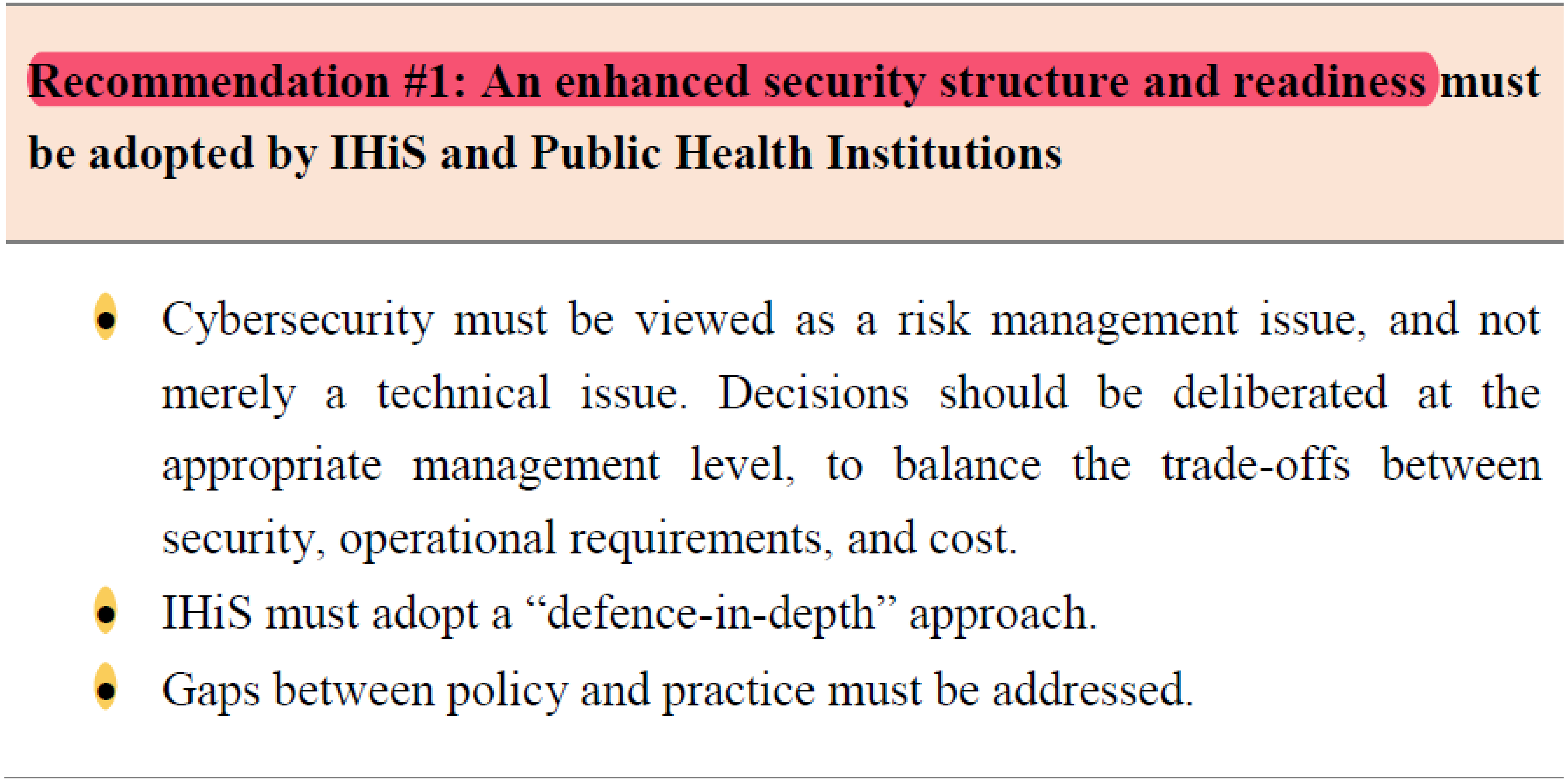
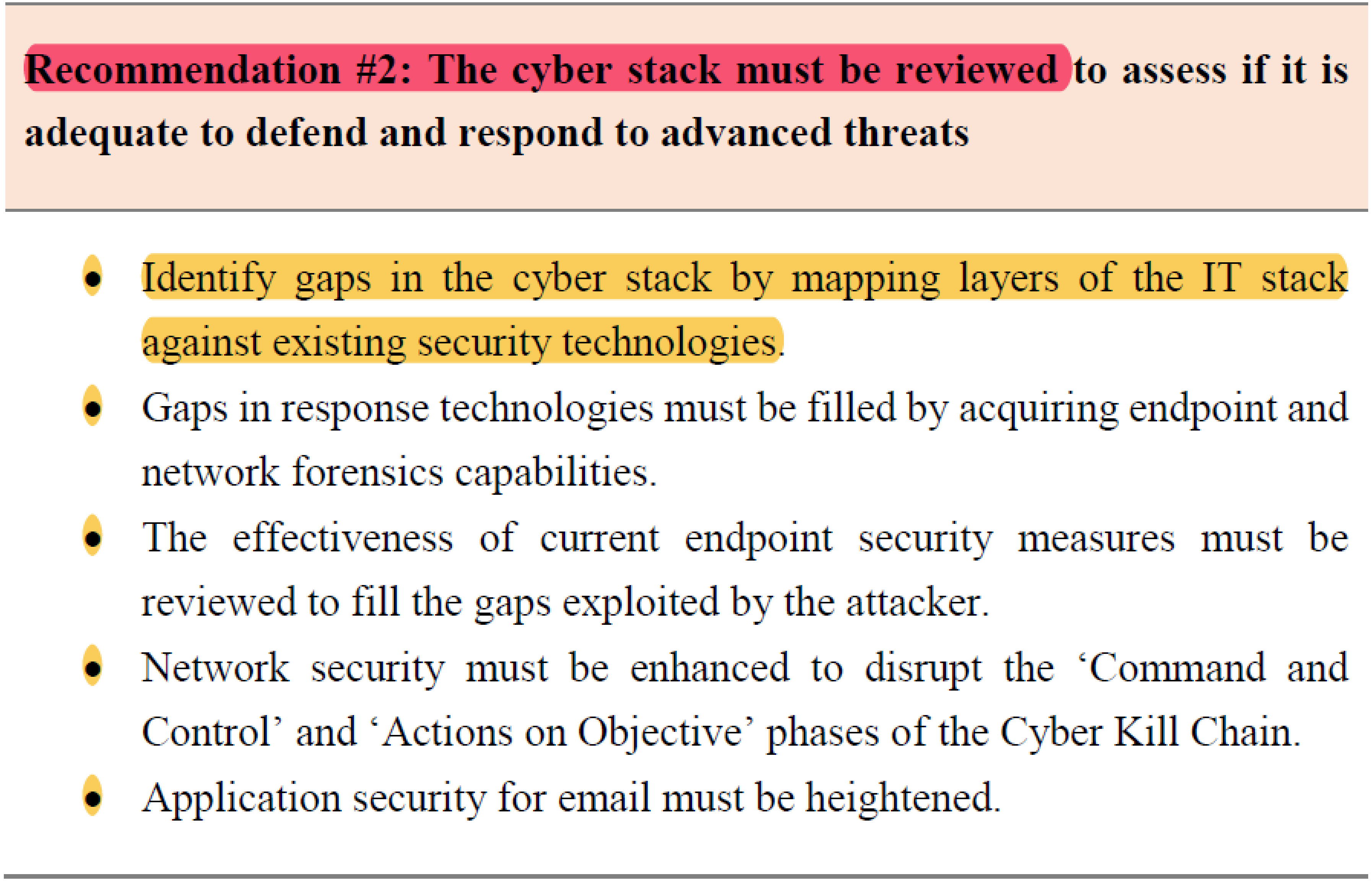


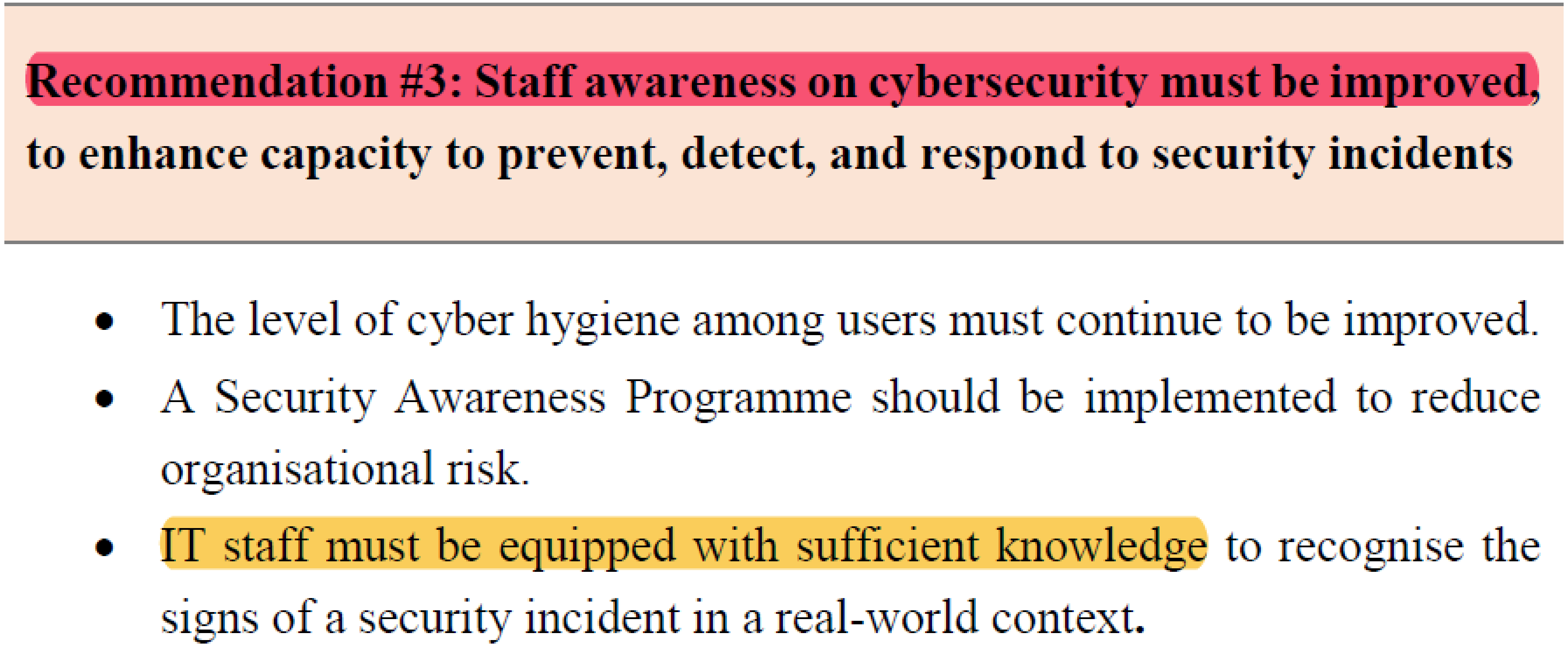
**Recommendation #1: An enhanced security structure and readiness must be adopted by IHiS and Public Health Institutions**

- Cybersecurity must be viewed as a risk management issue, and not merely a technical issue. Decisions should be deliberated at the appropriate management level, to balance the trade-offs between security, operational requirements, and cost.
- IHiS must adopt a “defence-in-depth” approach.
- Gaps between policy and practice must be addressed.



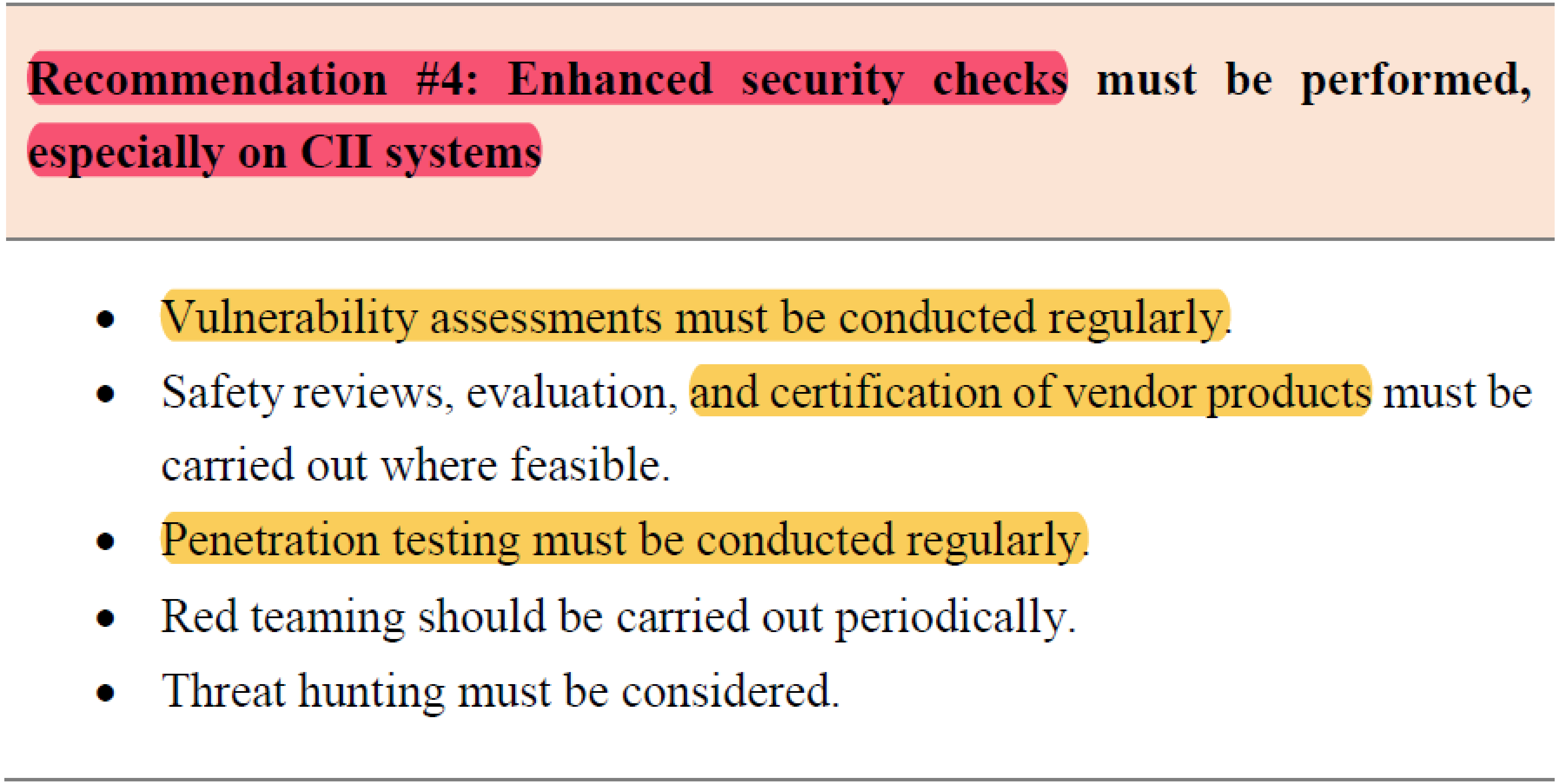
**Recommendation #2: The cyber stack must be reviewed to assess if it is adequate to defend and respond to advanced threats**

- Identify gaps in the cyber stack by mapping layers of the IT stack against existing security technologies.
- Gaps in response technologies must be filled by acquiring endpoint and network forensics capabilities.
- The effectiveness of current endpoint security measures must be reviewed to fill the gaps exploited by the attacker.
- Network security must be enhanced to disrupt the ‘Command and Control’ and ‘Actions on Objective’ phases of the Cyber Kill Chain.
- Application security for email must be heightened.



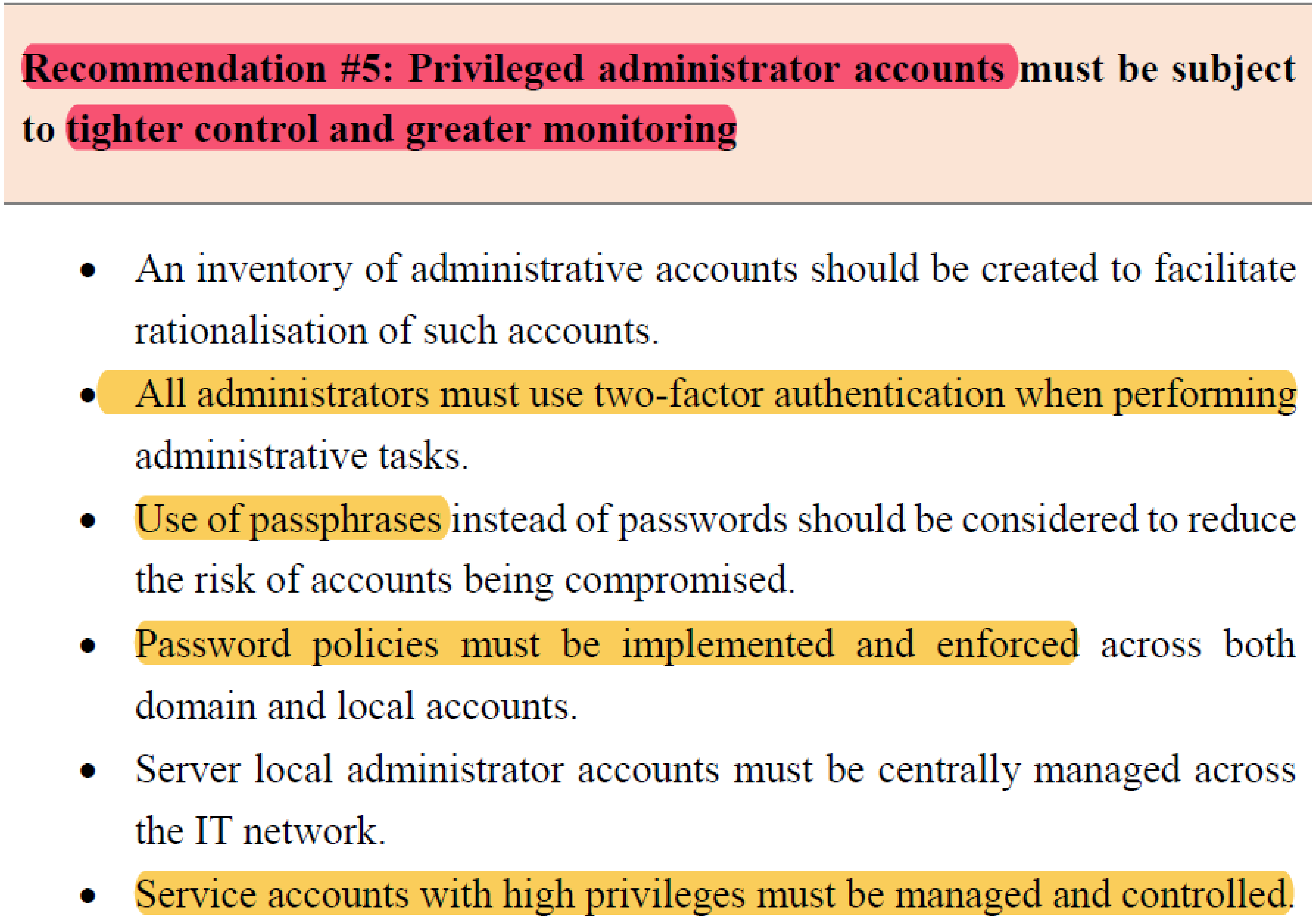
**Recommendation #3: Staff awareness on cybersecurity must be improved, to enhance capacity to prevent, detect, and respond to security incidents**

- The level of cyber hygiene among users must continue to be improved.
- A Security Awareness Programme should be implemented to reduce organisational risk.
- IT staff must be equipped with sufficient knowledge to recognise the signs of a security incident in a real-world context.



**Recommendation #4: Enhanced security checks must be performed, especially on CII systems**

- Vulnerability assessments must be conducted regularly.
- Safety reviews, evaluation, and certification of vendor products must be carried out where feasible.
- Penetration testing must be conducted regularly.
- Red teaming should be carried out periodically.
- Threat hunting must be considered.



**Recommendation #5: Privileged administrator accounts must be subject to tighter control and greater monitoring**

- An inventory of administrative accounts should be created to facilitate rationalisation of such accounts.
- All administrators must use two-factor authentication when performing administrative tasks.
- Use of passphrases instead of passwords should be considered to reduce the risk of accounts being compromised.
- Password policies must be implemented and enforced across both domain and local accounts.
- Server local administrator accounts must be centrally managed across the IT network.
- Service accounts with high privileges must be managed and controlled.