Question 2.6 How can impact analysis and mitigation be conducted for cyberattacks in the power system operational environment?

Impact analysis and mitigation be done in three stages.

Identifying critical infrastructure: Need for the comprehensive analysis on threat scenarios and prioritize attack risks based on their expected outcomes on system operation.

Majorly, the critical systems in the power system are grid inverters, utility-to-device communication channels, physical interfaces, substation circuit breakers/reclosures, and controllers. Gaining access to any of these assets can enable an adversary to manipulate the generated or stored energy, cause switch disconnections altering the system topology, false trips, feeder over loadings, voltage-frequency violations, damage protection equipment, or inflict system instabilities.

Assigning proper Score for each probable attacks: There is a need for relative metric / risk score where its calculations should involve the factors like, severity, risk probability, commercial impact, stability impact.

Security operations center: Should comply NISTIR 7628,NERC critical infrastructure protection (CIP), ISA99, IEEE 1402 (for physical security), etc.

Although the recommendations discussed in such standards can contribute towards effectively protecting critical infrastructure and power systems, they serve as security recommendations with limited enforcing capabilities therefore, complimentary security assessments should also be performed,

Necessary tools (offline) be required in the control centre to run the simulations for different cases by the operator and administered/prepared a defense mechanism to such attacks.