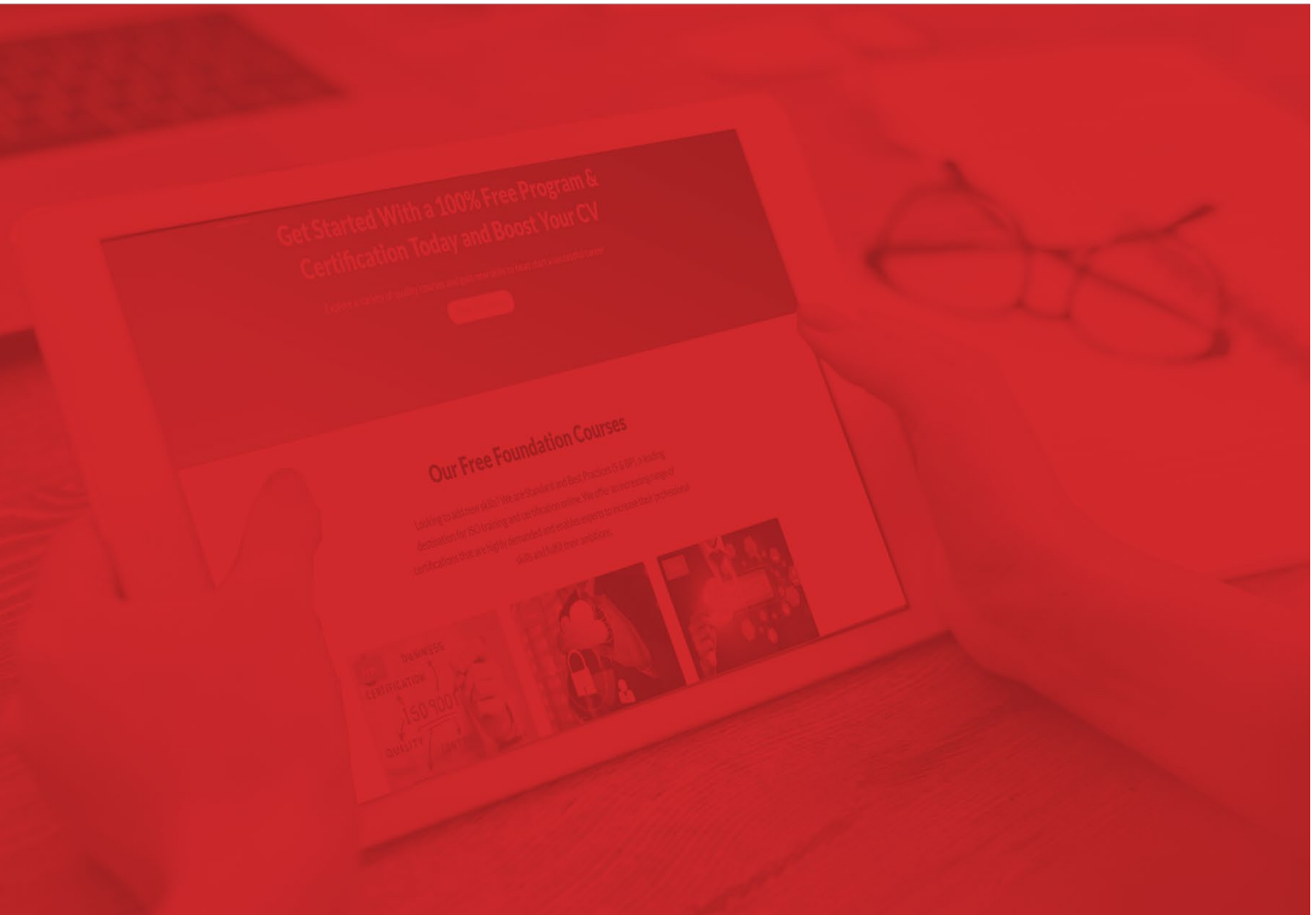
...global validation

SBP ISO 27001:2022 (ISMS) LEAD AUDITOR COURSE- CASE STUDIES



ISO 27001:2022 (ISMS) LEAD AUDITOR CASE STUDIES

CASE STUDY #1

XYZ Financial Services

XYZ Financial Services is a medium-sized financial institution that handles sensitive financial information for its clients. They recently implemented an ISO 27001 Information Security Management System (ISMS) to safeguard their data and ensure compliance with regulatory requirements.

Audit Focus Areas:

1. Information Security Policy
2. Risk Assessment and Treatment
3. Access Control
4. Incident Response and Reporting
5. Monitoring and Measurement

Scenario: During the audit, the audit team discovers that XYZ Financial Services has a comprehensive Information Security Policy in place. However, they observe that the policy hasn't been effectively communicated to all employees. Additionally, the risk assessment process is found to be outdated, and some critical assets are not adequately protected. The audit team also identifies a gap in the incident response plan.

Tasks for Trainees:

1. Classify the non-conformities identified into which is a Major or Minor NC.
2. Propose corrective actions for the identified gaps.

CASE STUDY #2

ABC Healthcare Solutions

ABC Healthcare Solutions is a healthcare technology company that stores and processes sensitive patient information. They have recently undergone an expansion and implemented ISO 27001 to ensure the security of patient data and maintain the trust of their clients.

Audit Focus Areas:

1. Asset Management
2. Information Classification
3. Physical and Environmental Security
4. Supplier Relationships
5. Compliance

Scenario: During the audit, the team discovers that ABC Healthcare Solutions lacks a comprehensive asset management system, leading to difficulties in tracking and managing IT assets. Information classification procedures are in place, but employees are not consistently applying them. Physical security controls,

especially in the server room, are found to be inadequate. Additionally, there are concerns regarding the assessment of suppliers' security practices, and there is uncertainty about compliance with legal and contractual requirements.

Tasks for Trainees:

1. Evaluate the effectiveness of the asset management system and propose improvements.
2. Classify the non-conformities identified into which is a Major or Minor NC.
3. Recommend actions to address any identified gaps.

CASE STUDY #3

PQR Services

Background: PQR Services is a consulting firm that recently obtained ISO 27001 certification for its information security management system (ISMS). The organization provides services related to data analytics and has a significant client base.

Scenario: During the audit, you observe that PQR Services has conducted a risk assessment, but the controls implemented to mitigate identified risks are not consistently monitored and reviewed. Additionally, there is no evidence of regular testing and validation of the incident response plan.

Tasks:

1. What non-conformities can you identify in the scenario given?

CASE STUDY #4

LMN Corporation

Background: LMN Corporation is a manufacturing company that recently started the process of implementing ISO 27001 to enhance its information security practices. The organization handles sensitive customer data and proprietary information.

Scenario: During the audit, you find that LMN Corporation has established an information security policy, but there is no evidence of a systematic process for identifying and assessing information security risks. Additionally, there is a lack of documented procedures for secure disposal of obsolete hardware containing sensitive information.

Tasks:

1. In your closing meeting, recommend actions to address any identified gaps.