SOFEMA AVIATION SERVICES

Workshop Task: Cyber Risk Identification within Your Organization

Objective:

The purpose of this task is to enable participants to quickly identify key cyber risks within their organization, assess associated vulnerabilities, and evaluate the potential impact on aviation safety. The goal is to improve the organization's ability to recognize and mitigate cyber threats.

Duration:

- Task Duration: 15–20 minutes (in groups)
- Presentation Duration: 5 minutes per group

Group Size:

- Groups of 4 participants (mixed functional roles where possible)

Instructions:

Each group will:

1. Identify cyber threats within the organization.
2. Identify vulnerabilities that could allow these threats to materialize.
3. Assess the likelihood and impact of each threat exploiting the vulnerability.
4. Summarize key risks and propose initial mitigation strategies.

Task Breakdown:

Step 1: Identify Cyber Threats (3–4 minutes)

- Discuss and list up to 3 key cyber threats that could realistically affect your organization.
- Focus on the following threat categories:
  - Cyber Attacks – Hacking, malware, phishing, ransomware, denial of service (DoS).
  - Insider Threats – Unauthorized access, data leaks, employee sabotage.
  - System Failures – Software malfunctions, hardware failures, network disruption.
  - Supply Chain Threats – Vulnerabilities introduced by external service providers.
  - Human Error – Poor password hygiene, misconfigurations, accidental deletions.

Step 2: Identify Vulnerabilities (3–4 minutes)

- For each identified threat, identify the vulnerability that could enable the threat to materialize.
- Focus on areas such as:
  - IT Infrastructure – Weak firewalls, unpatched systems.
  - Data Protection – Weak access controls, lack of encryption.
  - Human Factors – Poor training, lack of security awareness.
  - Third-Party Interfaces – Poor contract terms, lack of security SLAs.

Step 3: Assess Likelihood and Impact (5 minutes)

1. For each threat-vulnerability combination, assess:
   - Likelihood – How likely is the threat to materialize?
   - Impact – How severe would the consequences be?

Use the following scale:

Likelihood	Definition
High	Likely to occur
Medium	Could occur
Low	Unlikely to occur

Impact	Definition
High	Significant safety or operational impact
Medium	Moderate disruption, some operational impact
Low	Minor or negligible impact

Step 4: Develop Initial Mitigation Strategies (3–4 minutes)

• For each identified high or moderate risk, suggest one or two mitigation actions.

Examples of mitigation strategies:

- Introduce multi-factor authentication.
- Improve staff training on email security.
- Upgrade firewall and network monitoring.
- Improve access control policies.

Summary Template:

Threat	Vulnerability	Likelihood	Impact	Risk Level	Mitigation Strategy
Phishing attack	Weak email security	High	Medium	High	Introduce multi-factor authentication
Ransomware attack	Outdated firewall	Medium	High	High	Upgrade firewall settings
Insider threat	Weak access control	Low	Medium	Moderate	Strengthen access control policies

Group Presentations (5 Minutes per Group):

- Each group will present:
  - ✅ The top 3 threats identified.
  - ✅ The associated vulnerabilities.
  - ✅ The likelihood and impact.
  - ✅ The suggested mitigation strategies.

Success Criteria:

- Each group must identify at least three realistic cyber threats.
- Each threat must be linked to a specific vulnerability and risk level.
- Each group should propose at least one mitigation strategy for each high-risk threat.

Takeaway:

This task will help participants understand how to identify and assess cyber threats, recognize vulnerabilities, and prioritize mitigation strategies—directly improving the organization's information security resilience.