EASA Cyber Security - Guidance on Performing a Product and Part Security Risk Assessment (PISRA)

Sofema Aviation Services (SAS) www.sassofia.com considers key aspects in relation to the process for the Security Risk Assessment identified in ED-202A Section 2.1.1(PISRA)

ED-202A Section 2.1.1 is an acceptable means of compliance for performing the PISRA for products and parts under Annex I (Part 21) to Regulation (EU) No 748/20121.

Additional Guidance material for the PISRA can be found in ED-203A.

Guidance on Performing a Product and Part Security Risk Assessment (PISRA)

- The process outlined in ED-202A Section 2.1.1 is recognized as an acceptable means of compliance (AMC) for performing the Product and Part Security Risk Assessment (PISRA) under Annex I (Part 21) to Regulation (EU) No 748/2012.

Here we consider Below is a step-by-step explanation and guidance on implementing this process effectively, referencing ED-203A for detailed methodologies and best practices.

Understand the Context and Scope - PISRA Objective: The goal is to assess and mitigate security risks associated with aviation products, parts, and appliances during design and production.

Compliance Framework: Ensure alignment with EASA Part 21 requirements and any additional specific security considerations mandated by EU Regulation 748/2012.

- Achieving compliance with EASA Part 21 requires a robust understanding of the regulatory framework, integration of security risk management into organizational processes, and alignment with PISRA methodologies. In addition to ensure alignment with Safety Management System Objectives.
- Using ED-202A and ED-203A as reference frameworks ensures that your approach meets both the technical and procedural expectations of these regulations.
- Regular audits, training, and continuous monitoring are critical to maintaining compliance.

Process Overview per ED-202A Section 2.1.1

The PISRA process involves **several main steps** to evaluate and address potential security threats:

Establish System Boundaries:

Establishing system boundaries is essential for a focused and effective security risk assessment. By identifying the product or part under assessment and defining its functional, operational, and regulatory environments, organizations can ensure that all relevant risks are addressed while

maintaining compliance with regulatory standards. Clear boundaries set the stage for successful risk identification, mitigation, and validation.

- Identify the product or part under assessment.
- Define its functional, operational, and regulatory environment.
  - Defines the real-world conditions under which the product or part will function.
  - Temperature, pressure, vibration, and other environmental factors.
  - Describe where and how the system will be used (e.g., in the cockpit, ground operations, maintenance facilities).
  - Define how users or operators interact with the system.
  - Consider how the system interacts with external entities (e.g., third-party systems, regulatory bodies).

Identify Security Objectives:

- Determine the critical assets requiring protection.
- Outline the security goals to ensure asset confidentiality, integrity, and availability.

Identifying security objectives by determining critical assets and aligning with Confidentiality, Integrity, and Availability principles ensures a targeted and effective approach to securing aviation products and parts.

This step lays the foundation for the entire PISRA process, enabling organizations to develop appropriate mitigations and achieve regulatory compliance.

Threat Identification:

- Identify potential threats relevant to the product or part.
- Use industry best practices (refer to ED-203A) to catalog threats systematically.

Vulnerability Assessment:

- Analyze weaknesses in the product, part, or associated systems that could be exploited by threats.
- Consider vulnerabilities during the design, manufacturing, and operational phases.

Risk Assessment - Evaluate the impact of potential security threats exploiting identified vulnerabilities.

Apply risk assessment methodologies (refer to ED-203A for detailed tools and techniques).

Select Appropriate Risk Assessment Methodologies - ED-203A outlines multiple tools and techniques for assessing risks. The choice depends on the complexity of the system and the nature of the risks. Below are commonly used methodologies:

Fault Tree Analysis (FTA) - Identify root causes of security failures by analyzing a top-level security breach.

- **Steps**:
  - Define the undesired top event (e.g., unauthorized access to a critical system).
  - Break down the event into its contributing factors, using a tree structure.
  - Analyze the probability of each contributing factor.

When to Use: For highly structured systems where understanding failure chains is critical.

Event Tree Analysis (ETA) - Evaluate potential outcomes of an initiating event, focusing on the effectiveness of mitigation measures.

- **Steps**:
  - Define an initiating event (e.g., malware intrusion).
  - Map possible events branching from the initial one.
  - Calculate probabilities for each branch and assess their consequences.

When to Use: To analyze sequences of events and evaluate risk mitigation effectiveness.

Failure Mode and Effects Analysis (FMEA) - Identify potential failure modes, their causes, and consequences.

- **Steps**:
  - List all components and functions.
  - Identify failure modes for each component.
  - Assess the severity, occurrence likelihood, and detection probability.
  - Calculate the Risk Priority Number (RPN) = Severity × Occurrence × Detection.

When to Use: For systematic identification and prioritization of risks in complex systems.

Attack Tree Analysis - Analyze potential attack paths and their likelihood of success.

- **Steps**:
  - Define a goal (e.g., compromise of sensitive data).
  - Identify all possible attack paths leading to the goal.
  - Assign likelihood and impact scores to each path.

When to Use: For analyzing cybersecurity threats and their pathways.

E. Hazard and Operability Study (HAZOP) - Examine deviations in the system design or operations that could lead to security risks.

- **Steps**:
  - Define system operations or design.
  - Identify deviations (e.g., unauthorized system access).
  - Assess the causes, consequences, and safeguards for each deviation.

When to Use: For exploring potential deviations in highly complex systems.

Risk Matrices - Provide a visual representation of risks based on likelihood and severity.

- **Steps**:
  - Define severity levels (e.g., negligible to catastrophic).
  - Define likelihood levels (e.g., unlikely to almost certain).
  - Plot each risk on the matrix to prioritize them.

When to Use: For straightforward prioritization and decision-making.

Mitigation Strategies:

- Develop security measures to mitigate identified risks.
- Prioritize mitigations based on risk level and feasibility.

- Effective mitigation strategies require developing targeted security measures to address specific risks and prioritizing those mitigations based on risk level and feasibility.

- By balancing risk severity, implementation cost, and operational impact, organizations can ensure resources are used efficiently while maintaining compliance and securing their products and parts against threats.

- **Design Mitigation Measures**:
  - Implement measures to address vulnerabilities, such as:
    1. Software patches.
    2. Hardware redundancies.
    3. Operational controls.

Document Findings:

- Maintain detailed documentation of the entire PISRA process, including identified risks, mitigation measures, and residual risk levels.

Leveraging Guidance Material in ED-203A - provides practical guidance and methodologies to enhance the PISRA process:

Threat and Vulnerability Analysis:

Use threat libraries and industry-standard vulnerability databases to strengthen identification efforts.

- **Threat Cataloging**:
    - Use threat libraries or standards such as ED-203A to identify known security threats.
    - Include threats relevant to:
        - Cybersecurity.
        - Physical security.
        - Operational disruptions.
- **Consider Threat Sources**:
    - Internal threats (e.g., insider threats).
    - External threats (e.g., hackers, environmental conditions).
- **Scenario Development**:

Develop realistic threat scenarios for your product or part

Risk Assessment Frameworks:

- Employ models such as **Fault Tree Analysis (FTA)**, **Event Tree Analysis (ETA)**, or **Failure Mode and Effects Analysis (FMEA)** for systematic evaluation.

Mitigation Validation:

- Ensure mitigations are effective through simulation, testing, or peer review.

Mitigation validation through simulation, testing, and peer review is essential to ensure that security measures effectively address identified risks without introducing new vulnerabilities. By using these methods iteratively and incorporating real-world conditions, organizations can build robust and compliant security systems while maintaining confidence in their effectiveness.

- **Residual Risk Management**:
    - Implement procedures for monitoring and managing risks that cannot be fully mitigated.

Best Practices

- **Engage Multi-Disciplinary Teams**: Include experts from security, design, production, and operations.
- **Iterative Approach**: Perform PISRA iteratively throughout the design and production lifecycle to address emerging risks.
- **Alignment with SMS**: Integrate PISRA into the organization’s Safety Management System (SMS) to ensure comprehensive oversight.

Conclusion

The PISRA process guided by **ED-202A Section 2.1.1** and supported by **ED-203A** provides a robust framework for ensuring the security of aviation products and parts.

Compliance with this process not only meets regulatory requirements but also strengthens the overall security posture of the organization.

Next Steps

See the following 2 day course https://sassofia.com/course/implementing-information-cyber-security-program-easa-part-145-organization-2-days/ for comments or questions please email team@sassofia.com