BG ISMS Information

Review of the State Safety Programme of the Republic of Bulgaria (2024 edition) that touches Information & Cyber Security and how it aligns with EASA expectations.

What the document covers (scope)

- The SSP is a safety-management policy document aligned with ICAO Annex 19 and the EU/EASA system (EPAS, EU basic & implementing regulations). It is not an information-security manual; its treatment of information/cyber topics appears where they intersect with safety risk management and oversight.

Cybersecurity: how it's positioned

- Policy & goals. "Cybersecurity" is named alongside safety and security as a key threat that organizations must identify and address within their Safety Management Systems (SMS); risk management by both CAA and organizations explicitly includes cybersecurity risks. This sets an expectation that cyber risk is managed within the safety framework (hazard/threat identification, assessment, mitigation).
- **Safety–security interplay.** Where safety and security are interdependent, competent authorities must cooperate, including on cybersecurity, and react immediately to unlawful-interference concerns. This anchors cyber within coordinated state oversight.

Information management (confidentiality, reporting, sharing)

- Occurrence data protection & Just Culture. The SSP stresses confidentiality, appropriate use of occurrence information, and protection of sources under Regulation (EU) 376/2014, within a Just Culture climate. This is a foundational "information protection" control for safety data.
- Systems & tools. It references ECCAIRS as the EU system for collection, storage, analysis, and exchange of occurrence data—again highlighting governance around safety information.
- Collection/analysis/exchange. The SSP mandates continuous collection, analysis, and timely dissemination of safety information (incl. via EASA Safety Information Bulletins), with organizations required to take immediate action where needed. This is information-flow governance supporting risk control.

- **External information outreach & competence.** It also calls for external training/exchange and publishes principles of safety management on the CAA website—another aspect of controlled safety-information communication.

Where EASA alignment is made explicit

- The SSP ties Bulgaria's system to EASA's EPAS and the EASA Safety Risk Management (SRM) process, requiring national uptake of EPAS measures and organizational implementation where applicable.
- It points to EU implementing rules that embed SMS across domains (e.g., Air Ops 965/2012, Airports 139/2014, ATM/ANS 2017/373), making the SMS the vehicle that must also address cyber threats as defined in the policy goals.

What the SSP does not do (gap note)

- The document does not set out a dedicated Information Security Management System (ISMS) or detailed cyber-controls; "cybersecurity" is recognized at policy/oversight level, but there's no prescriptive Part-IS/ISMS framework in the text. In other words, the SSP tells organizations to treat cyber as a safety threat inside the SMS, but it does not enumerate specific information-security requirements or controls beyond data-protection rules for safety occurrences.

Practical takeaways for EASA-style compliance

Based on the SSP's direction—and consistent with how EASA expects organizations to manage non-traditional safety threats—organizations should ensure that:

1. **Cyber risks are in the SMS:** include cyber in hazard/threat registers, risk assessments, and change management; track safety performance impacts and mitigations.
2. **Safety–security coordination is formalized:** define interfaces between safety, security, and IT/OT teams; establish protocols with the CAA for issues that straddle safety and security (including cyber).
    - **Information Technology (IT) -** Digital systems that support the business and compliance side of your operation.
    - **Operational Technology (OT) -** Hardware/software that monitors or controls physical processes

3. **Safety data governance is robust:** maintain Just Culture protections, confidentiality of occurrence information, and proper use of ECCAIRS; train staff on handling safety information.
4. **Information dissemination is controlled yet timely:** monitor EASA SIBs and other advisories; issue internal bulletins and take immediate action where risk is identified.
5. **Domain rules remain the anchor:** ensure your cyber-related mitigations are reflected in the SMS arrangements required by the applicable EU implementing rules for your domain (Ops, Airport, ATM/ANS, Maintenance, etc.).

Bottom line

- The SSP recognizes cybersecurity as a strategic safety threat and expects it to be managed within the SMS and through coordinated authority action, while protecting safety information under EU occurrence-reporting rules.
- It does not prescribe an ISMS or detailed cyber controls; any organization seeking full EASA-style information & cyber-security compliance should map cyber hazards into the SMS, ensure robust safety-data governance, and align their domain approvals with EU implementing rules, using the SSP's policies as the umbrella.

Gap-to-Action Checklist (EASA Part-IS, built into existing manuals)

A. Cite the rule set up front (add to "Regulatory Basis" in your manual)

- Implementing Regulation (EU) 2023/203 (Part-IS for organisations and authorities).
- Delegated Regulation (EU) 2022/1645 (Part-IS for DOA/POA/ADR/AMS; provides the overarching construct).
- AMC/GM to Part-IS — ED Decision 2023/008/R (and related 009/R, 010/R) — application from 22 Feb 2026.
- Easy Access Rules for Information Security (rev. June 2024) — consolidated IR/DR + AMC/GM.

One sentence to insert: “This organisation implements EASA Part-IS requirements within its existing management system; the ISMS scope, processes and controls are documented herein and in the referenced appendices.”

B. Management system inserts (what to add/strengthen, section by section)

1) Policy & Scope (front of MOE/CMM)

- Signed Information Security Policy linking cyber/information risk to aviation safety objectives and SMS. Name the Accountable Manager as ultimately accountable.
- Scope statement: what assets, processes, systems and interfaces are covered (include OT/ICS on the ramp/hangar, maintenance IT, records, e-logs, e-orders, vendor connections). Clarify any exclusions/derogation logic if applicable.

2) Roles, Responsibilities, Competence

- Appoint an Information Security Lead (function can be part-time in small orgs) with authority to drive risk treatment and incident response; show interfaces with Compliance Monitoring and Safety Manager.
- Add a competence & training paragraph: awareness for all, task-specific training for the IS Lead/IT, and management briefings; note alignment to AMC Appendix II / NIST CSF mapping for skills coverage.

3) Risk Assessment & Risk Acceptance (tie to SMS)

- Define an information-security risk method that evaluates safety impact (not just confidentiality/integrity/availability in IT terms). Include risk criteria, acceptance by management, and SMS links (hazard/threat register, change mgmt).
- Maintain an Asset & Interface Inventory (aircraft data paths, M&E systems, tooling with software/firmware, remote access, vendor portals). Classify safety-critical items.

4) Controls & Operational Measures (keep pragmatic for small orgs)

- **Access control & identity**, secure configuration & patching, malware protection, segmentation for OT/ICS, backups/restore tests, and media handling (portable devices into maintenance areas).

    - Industrial Control Systems (ICS) - Think of OT as the operational environment; ICS is the control stack within it.

- **Change management** for software/firmware affecting maintenance effectiveness or airworthiness data (link to existing MOE change process). EASA
- **Records integrity/availability** for continuing airworthiness and maintenance releases (tie to MOE record-keeping).

5) Suppliers & Subcontractors (very visible to inspectors)

- Add a clause to your **procurement/contracting**: suppliers performing **information-security management activities** must meet Part-IS expectations; capture due diligence, security clauses, and right of audit. (Ref. **IS.I.OR.235** scope for suppliers.)
- For other suppliers (not performing IS management activities), show proportionate controls via **IS.I.OR.205** (risk-based oversight).

6) Event Detection, Incident Reporting & Recovery

- Define **event monitoring**, **incident classification** (what makes it an "information security incident with potential safety impact"), **24/7 contact chain**, and **escalation** into the SMS occurrence process where relevant.
- State the **notification path to the competent authority** under Part-IS (and, where applicable, how this interfaces with EU 376/2014 safety occurrence reporting). Keep a simple flowchart.
- Include **business continuity & disaster recovery targets** (RTO/RPO) for safety-relevant systems; test at least annually and minute outcomes.

7) Monitoring, Internal Audit, Management Review

- Add **Part-IS to your compliance monitoring plan**; audit annually (or on a risk basis). Track findings like any other regulatory non-conformity.
- Extend **management review** to include IS **KPIs/metrics**: incident stats, patching latency for safety-relevant systems, supplier issues, training coverage, open risk treatments.

8) Integration stance (make this explicit once)

- One paragraph that your **ISMS is integrated** with safety/quality/compliance and **not a standalone** system — perfectly acceptable for small orgs.

C. Appendices to create (kept lean for small orgs)

1. **ISMS Scope & Asset Register** (incl. external interfaces).
2. **Risk Register (safety-centric)** with treatment plans and acceptance signatures. EASA
3. **Supplier & Subcontractor Dossier** (classification vs. IS.I.OR.235, contracts/assurances, last review date).
4. **Incident Playbook** (decision tree, authority notification, comms templates).
5. **Training Matrix** (awareness + role-specific competence).
6. **BCP/DR Test Records** with lessons learned.

D. Evidence pack (what an inspector will expect to see quickly)

- Latest policy, scope, asset list, and top risks with safety impact identified.
- One recent change record showing security assessment for a system/tooling update.
- A supplier due-diligence file (questionnaire or clause set) for any IT/OT vendor touching maintenance processes.
- Incident drill minutes or a real case with timeline, classification, decisions, and (if applicable) authority notification.
- Internal audit report covering Part-IS clauses and a management review extract with KPI trends.

E. Dates & dependencies to call out in your manual

- Note explicitly that the AMC/GM apply from 22 February 2026 (you're already implementing and monitoring ahead of time).
- Mention relationship with NIS2/ISO 27001: alignment is helpful but does not equal Part-IS compliance; aviation-safety context and specific Part-IS tasks still apply.

Next Steps

Sofema Aviation Services & Sofema Online provide Information & Cyber Security Regulatory Training for Operators – CAMO,s and Part 145 as Classroom, Webinar and Online Training. Please see www.sassofia.com, www.sofemaonline.com or email team@sassofia.com