Checklist for EASA ATO ISMS & Cyber Compliance

Under EASA regulations—specifically Commission Implementing Regulation (EU) 2023/203 (Part-IS) and Regulation (EU) No 1178/2011 (Part-ORA, including ORA.GEN.200A)—EASA-approved Approved Training Organisations (ATOs) are required to establish, implement, and maintain an Information Security Management System (ISMS) integrated with their operational Safety Management System (SMS).

1. Governance, Leadership & ISMS Integration (IS.I.OR.200 / ORA.GEN.200A)

Compliance Item	Regulatory Ref.	Verification & Audit Evidence
Accountable Manager Endorsement	IS.I.OR.200(a)(1) ORA.GEN.200(a)(2)	Signed, dated Information Security Policy endorsed by the Accountable Manager linking cyber resilience directly to aviation safety goals.
Designation of Responsible Person	IS.I.OR.240(a) IS.AR.225(a)	Formally appointed CISO or Common Responsible Person (CRP) with direct reporting access to the Accountable Manager and delegated budget/resources.
ISMS & SMS Integration	ORA.GEN.200A IS.I.OR.200(d)	Cross-functional integration of information security risks into the existing SMS (ORA.GEN.200) and Compliance Monitoring Function (CMF) / Organisational Review Programme.
Information Security Management Manual (ISMM)	IS.I.OR.250 ORA.ATO.130	Approved ISMM or consolidated ATO Management System Manual documenting key cyber processes, roles, and document control procedures.
Proportionality & Exemption Review	IS.I.OR.200(e) AMC1 ORA.GEN.200(a)(6)	For small or non-complex ATOs, documented risk-based justification for a simplified ISMS or formal authority approval if requesting exemption.

2. Asset Mapping & ISMS Scope Delineation (IS.I.OR.205)

- **Synthetic Training Devices & FSTDs**: Map all Flight Simulation Training Devices (FFS, FTD, FNPT, BITD), visual/motion computers, device software updates, and Qualification Test Guide (QTG) databases.
- **Student, Exam & Training Records**: Identify and secure all digital student logbooks, progress tracking platforms, Area 100 KSA assessment records, and theoretical exam software interfaces.
- **Flight Operations & Dispatch Infrastructure**: Map scheduling systems, Flight & Duty Time Limitations (FTL) tracking software, and Electronic Flight Bag (EFB) weather/navigation data pipelines.
- **Aircraft Continuing Airworthiness Interfaces**: Map software data loaders, digital technical logs, Minimum Equipment List (MEL) tracking software, and maintenance interfaces for the ATO flight fleet.
- **Supply Chain & Interface Mapping**: Document external data exchange channels with contracted FSTD operators, third-party CAMO/Part-145 maintenance providers, and distance-learning ground school platforms.

3. Aviation Safety-Centric Cyber Risk Assessment (IS.I.OR.205 / IS.I.OR.210)

- **Threat Scenario Identification**: Identify realistic ATO threat scenarios (e.g., FSTD flight model or visual database corruption, EFB NavData spoofing, unauthorized alteration of student qualification/flight records, malware introduction via maintenance USB data loaders).
- **Safety Impact Analysis**: Evaluate threat scenarios by mapping information security compromises directly to *aviation safety consequences* (bridging the Information Security Assessment Process with the SMS Safety Assessment).
- **Risk Register & Severity Matrix**: Maintain a centralized Risk Register classifying risks based on occurrence potential and safety severity (High, Medium, Low).
- **Risk Treatment Plan Execution**: Implement time-bound risk treatment controls for unacceptable risks, verifying that security controls do not introduce new operational safety hazards.
- **Interface Risk Alignment**: Share and align risk assessment data with interfacing third-party vendors and operators along the operational functional chain.

Action Area	Required Capability	Operational Requirement
Detection	Anomaly & Baseline Monitoring	Operational baselines to detect unauthorized system access, software tampering, or data manipulation in training/dispatch systems.
Internal Escalation	Reporting Scheme & Just Culture	Internal reporting mechanism integrated with ATO Just Culture principles to encourage reporting of cyber glitches and vulnerabilities.
Response Playbooks	Multi-Disciplinary Incident Protocols	Incident response playbooks connecting IT/cyber containment directly with the Head of Training (HT), Chief Flying Instructor (CFI), and Safety Manager.
External Reporting	Authority Notification	Procedures to report safety-impactful cyber incidents to the National Competent Authority (NCA) and EASA within required reporting windows under Regulation (EU) 2023/203 and Regulation (EU) No 376/2014.
Recovery	Safe State Restoration	Business continuity and data backup procedures to restore FSTD, dispatch, and student records to a verified safe operational state within set Recovery Time Objectives (RTO).

5. Personnel Vetting, Competence & Role-Specific Training (IS.I.OR.240)

- **Personnel Trustworthiness & Background Checks**: Conduct documented identity verification and background vetting for staff and instructors possessing administrative access to critical systems or student records.
- **Written Security Acknowledgments**: Ensure all staff acknowledge their specific information security roles and operational guidelines in writing.
- **Flight Instructor (FI/TRI/SFI) Cyber Training**: Conduct role-specific training on GPS spoofing/jamming awareness, EFB data verification, and handling in-flight digital anomalies.
- **Maintenance & FSTD Engineer Cyber Training**: Train technical staff on secure software loading, USB data loader sanitization, and network isolation of synthetic flight devices.

- **Administrative & Ground Staff Cyber Training**: Deliver training focused on credential protection, anti-phishing, student database integrity, and Data Loss Prevention (DLP).

6. Supply Chain & Contracted Activities Oversight (IS.I.OR.235)

- **Pre-Contract Information Security Assessment**: Evaluate the cybersecurity maturity and ISMS capabilities of prospective contractors (e.g., third-party FSTD centers, cloud scheduling vendors, e-learning providers) prior to contract execution.
- **Contractual Cyber Clauses**: Enforce mandatory contractual provisions requiring suppliers to report cyber incidents, maintain security controls, and grant the ATO audit rights.
- **Supplier Compliance Auditing**: Regularly audit and monitor third-party contractors to verify ongoing compliance with the ATO's information security standards.

7. Record-Keeping & Continuous Improvement (IS.I.OR.245 / IS.I.OR.260)

- **ISMS Audit & Incident Record Retention**: Store all ISMS manuals, risk registers, audit reports, and incident logs in a secure, tamper-evident format for a minimum of 5 years.
- **Staff Qualification File Retention**: Retain individual staff cyber qualification, vetting, and training records for the duration of employment plus at least 3 years post-employment.
- **ISMS Effectiveness Metrics**: Track key performance indicators (KPIs) to evaluate ISMS operational performance and control effectiveness.
- **Annual ISMS Maturity Review**: Conduct annual management reviews and maturity assessments to identify operational gaps and drive continuous ISMS refinement.