Part-IS.EU

PART-IS Implementation Roadmap

Part-IS.EU

1 Introduction

This Implementation Roadmap provides compliance departments with a structured and practical guide designed to systematically achieve compliance with Part-IS regulations. It outlines essential tasks clearly and logically, supporting efficient implementation through recommended steps. This roadmap aims to simplify the compliance process, facilitating clear understanding, ease of use, and consistent application across your organisation.

Part-IS.EU

Table of Contents

Part-IS.EU

Assign Your Team

Establishing a clear and accountable team is one of the most important steps in building your Information Security Management System (ISMS). Regardless of your organisation's size, even if it's just one or two people, Part-IS requires key roles to be identified and assigned. This is your moment to assemble your own information security team, complete with clearly defined responsibilities and ownership.

Begin by assigning Task ownership. Every document, process or task in your ISMS should have a designated owner. This person is responsible for maintaining, updating, and being the go-to subject matter expert for their assigned material. When an auditor asks about a specific policy, plan, or register, you want to know exactly who to direct them to. Ownership creates accountability, and nothing ensures follow through like having your name attached to the document.

While it's tempting to assign responsibility to a team, it's strongly recommended to assign ownership to a specific individual. Assigning to a group often leads to unclear responsibilities, poor maintenance, and complications during audits.

Next, define your key information security roles. Complete the Roles and Responsibilities document using the structure below to assign individuals to each critical ISMS function formally:

- Accountable Manager: Holds overall responsibility for the ISMS and ensures that resources and authority are provided.
- Nominated Persons: Own implementation efforts within their operational domains (e.g., IT, Flight Operations, Maintenance).
- Compliance Monitoring Role: Conducts audits, verifies ISMS conformity, and tracks corrective actions.
- Common Responsible Person (CRP): Coordinates across departments where responsibilities overlap, ensuring alignment, risk management, and reporting.

These roles form the foundation of your Management Review Team, which acts as the governing body for your ISMS. This team will meet regularly to assess progress, approve changes, and oversee ongoing compliance, following the structured agenda

provided in the toolkit.

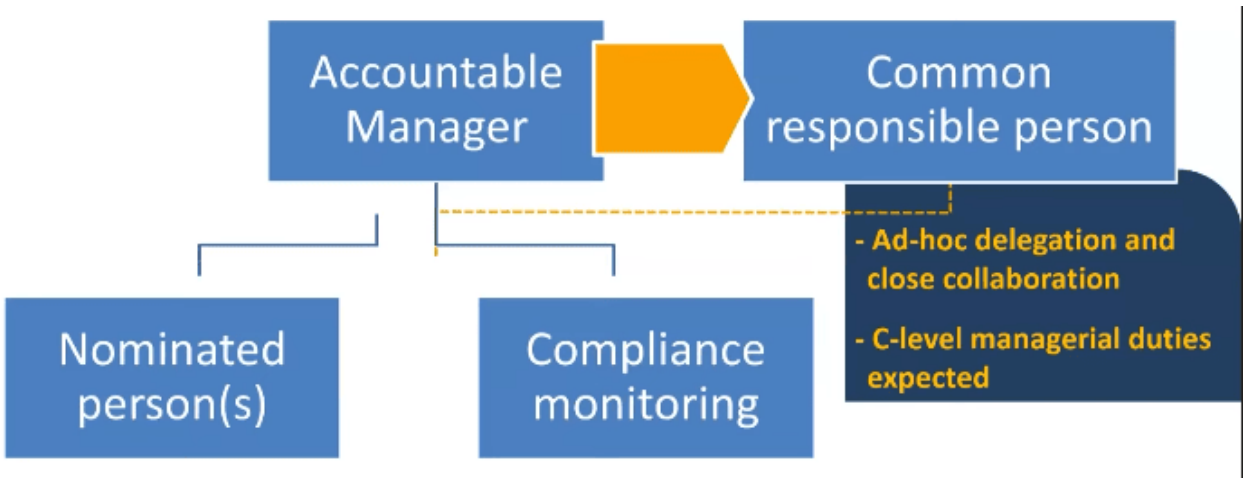
You should also assign owners to each of the main Part-IS tasks. While full implementation will take place in the next phase, assigning ownership now ensures subject matter experts are engaged early. Each task in the Part-IS structure represents a specific area of responsibility, spanning compliance, security, operations, and beyond.

Use an ISMS Accountability Matrix to:

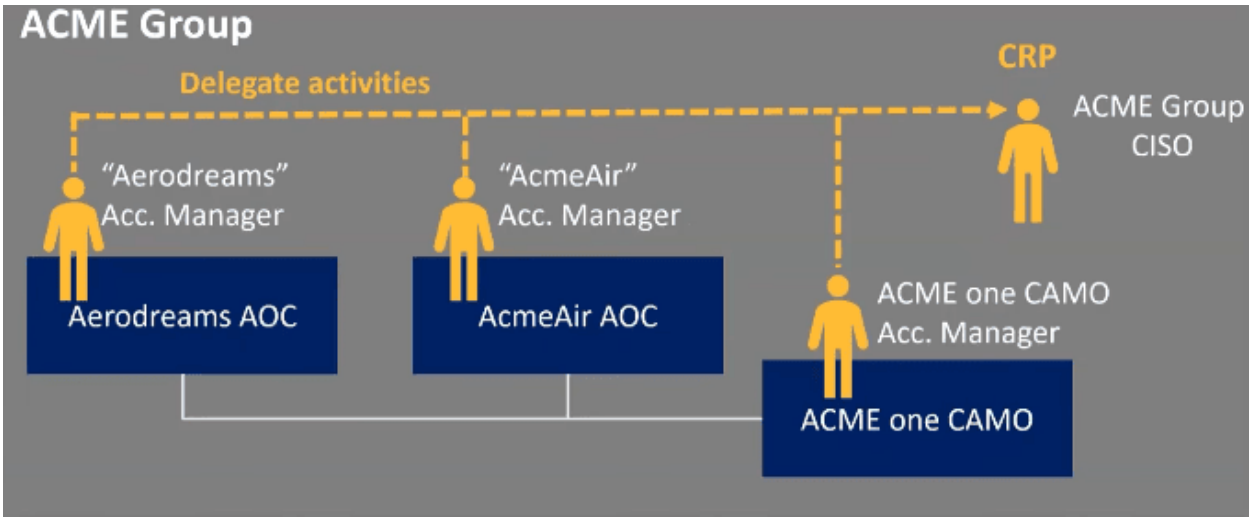
- Map each task or requirement
- Assign a clear primary owner (Responsible)
- Identify support and review roles where relevant

This proactive mapping enables smoother implementation, focused engagement, and audit readiness.

By clearly assigning people to roles, documents, and tasks from the outset, your ISMS gains clarity, structure, and momentum. The goal is not just to meet compliance, but to ensure ownership and engagement across the organisation. When accountability is embedded early, success becomes much more achievable.



Example Structure:



Understanding and Documenting Your Organisation and Assets

A critical early stage in establishing your Information Security Management System (ISMS) is forming a clear, documented understanding of who your organisation is, what it does, and how it interacts with information security risks and requirements. This creates the foundation on which the entire ISMS is built.

Start by preparing a concise organisational overview. This should explain the nature of your business, your key objectives, your strategic priorities, and your physical or operational locations. It should also describe how your ISMS supports and enhances these core elements, helping demonstrate that security measures are aligned with business goals, not isolated from them.

Next, define the context of your organisation. This means identifying all relevant stakeholders (internal and external), understanding their needs and expectations, and assessing internal and external issues that could influence your ISMS. Each issue should be reviewed to determine:

- Whether it poses a risk.

- Whether those risks have impact on aviation safety
- If it does, link it to your risk register.
- If it does not, document that it was considered and explain why it was ruled out.

This process shows thoroughness and helps provide traceability for auditors.

Once the context is clear, move on to documenting the scope of your ISMS. The scope defines what the system will cover, such as specific products, services, departments, or processes, and should be clearly aligned with what your customers expect you to protect. An accurate, justifiable scope helps ensure the ISMS is appropriately sized and resourced.

You must also identify all legal, regulatory, and contractual obligations relevant to your operations. These may include data protection laws, aviation safety requirements, cybersecurity legislation, and specific clauses in supplier or customer contracts. For each obligation, record:

- The title and reference of the requirement.
- The operational area it affects.
- The accountable role within your organisation.
- Any related risks recorded in the risk register.

With obligations documented, you'll need to establish an inventory of your information assets. Begin with a register of all physical and virtual devices that store, process, or transmit data. Include both organisation-owned and user-owned devices, especially if they connect to in-scope systems. The goal is to ensure visibility and appropriate control.

In parallel, create a register of your data assets. This should include databases, files, systems, and other data repositories, with details drawn from process documentation, technical architecture, or consultation with relevant teams.

You should also maintain a register of software assets, capturing all licensed applications used within the organisation. This supports not only compliance and

security, but also license management and intellectual property protection.

To ensure that your ISMS implementation aligns with the regulatory framework, complete an Applicability Tracking exercise. Review each requirement and determine whether it applies to your organisation. For requirements that do not apply, include a clear and defensible rationale. Update this document regularly as your operations evolve.

Finally, evaluate your third-party suppliers. These partners often introduce significant information security risks, so maintaining a detailed supplier register is essential. For each supplier:

- Confirm that there is a valid contract in place with security clauses.
- Where possible, obtain certifications or assurance statements.
- If assurance cannot be obtained, record and manage the associated risk appropriately.

This full picture - of your structure, scope, obligations, assets, and suppliers - forms the backbone of a well-documented ISMS and sets the stage for successful implementation and oversight under Part-IS.

Document Your Information Security Management System

Once your organisation is clearly defined, the next step is to document the Information Security Management System (ISMS) itself. This means articulating its purpose, structure, supporting resources, and how its performance is measured and improved over time. These elements form the operational backbone of your ISMS and are essential to demonstrate alignment with Part-IS.

Begin by establishing your Information Security Objectives. These define the intent behind your ISMS—why it exists, what it aims to achieve, and how it supports broader organisational goals. These objectives must remain consistent across all documentation, particularly in the Information Security Policy and Management Review meeting records. Each objective should have a clearly assigned owner, measurable outcomes, and criteria for evaluating performance over time. These

metrics serve as the foundation for tracking the ISMS's effectiveness and maturity.

Next, complete your Information Security Management Manual (ISMM). This document serves as a central reference, outlining the key components, structure, and operational boundaries of your ISMS. It brings together your governance model, control framework, and documentation into a single, accessible format for both internal and external stakeholders.

Equally important is the Competency Matrix. This tool demonstrates that your organisation has the skills and expertise required to operate the ISMS effectively. It should include all individuals with ISMS-related responsibilities, whether internal staff or external consultants. For each role, identify:

- Required competencies
- Current competency levels
- Gaps or areas for development
- Planned actions to close those gaps (e.g., training, certifications, recruitment)

This matrix also links directly to other foundational documents such as the Roles and Responsibilities register and the Accountability Matrix. A well-maintained competency matrix assures auditors that the ISMS is not only well-documented but also well-resourced.

Review your Information Classification Summary to ensure alignment with your information handling policies. While no action may be required at this stage, be familiar with this summary, as it will be shared during implementation and communicated across the organisation.

To measure how well your ISMS is functioning, develop and maintain an Information Security Measures Report. For each objective, define practical, relevant metrics that can be reported on monthly. These measures often derive from your operational processes—for example, the percentage of systems fully patched, antivirus activity logs, or the completion rate of security awareness training. Establish a reporting format that allows for consistent data entry and trend analysis. Historical reports should be retained and regularly reviewed as part of the Management Review process.

Together, these documents form the core of your ISMS. They define what you're working toward, how you're structured to achieve it, and how you will know whether you're succeeding - all essential components of a robust, compliant, and effective system. Fully aligned templates for each item are available in the Part-IS Implementation Toolkit.

Conduct Your Risk Review

Risk management is at the core of any effective Information Security Management System, and Part-IS places particular emphasis on identifying, assessing, and managing risks that may impact aviation safety. Conducting a structured risk review and maintaining a living risk register are fundamental to demonstrating both compliance and operational awareness.

Start by organising a dedicated risk review meeting. This should be held at least once a year and involve your Management Review Team along with any other individuals who can contribute valuable insights. The meeting functions as a collaborative workshop—reviewing known risks, exploring issues identified in your organisational context, and brainstorming new risks based on your evolving environment. This session should be clearly documented, with meeting minutes retained for audit purposes.

Following the meeting, update your organisation's risk register. The register must include:

- Any risks previously referenced in your Context of Organisation assessment
- All risks identified during the risk review meeting
- Clear links to any legal, contractual, or operational requirements that inform risk prioritisation

Ensure that your register reflects the current state of your risk environment and that each entry includes adequate detail, ownership, likelihood, impact, and planned treatment or controls. The register becomes a central tool for ongoing risk management and supports informed decision-making across your ISMS.

You should also have access to and understand your documented Risk Management Process. This process defines how risks are tracked, monitored, reviewed, and re-

evaluated over time, forming a continuous cycle that supports the maturity and responsiveness of your ISMS.

By completing a thorough risk review and maintaining an active register, your organisation can confidently demonstrate that risk-based thinking is embedded in its security culture - aligned with both Part-IS requirements and industry best practices.

Planning for Implementation and Oversight

A critical part of managing your Information Security Management System (ISMS) is not only executing security activities but also planning them in a structured, traceable manner. Planning brings intentionality, consistency, and accountability to your ISMS, and is an expectation under Part-IS. It also provides assurance to auditors that you are managing proactively, not reactively.

Begin with an audit plan. All ISMS components must be audited at least once annually - and certainly before any competent authority audit. Your plan should span a 12-month period and include all applicable areas of your organisation. Based on risk, some areas may require more frequent audits. Choose a cadence that suits your operational model - whether that means smaller, monthly audits or one or two comprehensive reviews per year. Ensure the plan is followed and that audit outcomes feed into your continual improvement process. For example, if a non-conformity is found and addressed, it may be appropriate to schedule a follow-up audit to verify the effectiveness of corrective actions.

Next, develop a communication plan. Communication is more than just good practice—it's a formal requirement. Plan how and when you will communicate ISMS-related matters across the organisation, and include key meetings such as Management Review, Security Operations and Risk Reviews planning. Document your communication activities for the year ahead, and retain evidence that they occurred. This might include meeting minutes, internal emails, newsletters, or screenshots of intranet updates. Auditors will expect to see both the plan and proof that it was carried out.

Lastly, complete your Information Security Management System (ISMS) Plan. This document outlines when and how operational changes to the ISMS will be made. The plan serves as your blueprint for ISMS evolution - tracking improvements, upgrades,

and key change milestones.

Together, these plans provide structure to your ISMS operations and evidence that your approach is systematic and future-oriented. Fully aligned templates are available in the Part-IS Implementation Toolkit.

Train Everyone

You need to train everyone on at least on basic information security, aviation safety and data protection and you need to evidence that they understood and accepted it. This is one place where a tool will do the heavy lifting for you as they come with prebuilt modules, have tests and quizzes built it to demonstrate understanding and come with reports that show who has completed the training. You should make sure that everyone has completed the basic training before the competent audit, and you should plan in additional training for the next 12 months. Remember that the basic training should be conducted and evidenced at least annually.

Implement Your Operational Processes

With planning complete and your ISMS structure in place, the next step is to operationalise your information security practices. This means turning documented intentions into day-to-day actions that are specific to your organisation - and more importantly, tailored to the aviation environment in which you operate.

Your operational processes are where policy meets practice. They show how your organisation actively protects critical systems, addresses aviation safety, manages data securely, and responds to incidents. These processes are not just internal tools - they also serve as key audit evidence demonstrating that your ISMS is functioning in real life, not just on paper.

Start by reviewing your aviation-specific operational needs. Focus on processes that ensure:

- Protection of critical data
- Secure access to systems such as air traffic control, flight ops platforms, or dispatch systems, etc

- Aviation-specific incident response procedures
- Risk Management Process
- Bow tie exercise to identify risks with potential aviation safety impact
- Internal and external reporting schemes
- Security of the entire supply chain relevant to your aviation services

These processes must reflect your organisation's role in the aviation ecosystem. That includes everything from handling operational and passenger data, to coordination with regulators and maintaining security across physical infrastructure like data centres and control rooms. Monitoring and traceability are essential.

Each operational process must be documented clearly, covering:

- Who is responsible for performing each task
- What systems and tools are used
- How activities are monitored, logged, and reported—especially in aviation-critical areas like flight planning, communications, and system integrity

This documentation should be structured in a way that supports both internal consistency and external audit readiness. Logs, procedures, approvals, and training records may all serve as acceptable evidence.

Auditors will expect to see proof that your processes are implemented and working, such as:

- Access logs for critical systems
- Change control records for operational platforms
- Incident reports and reviews specific to aviation contexts
- Results from system security scans and control monitoring

All of this must be reflected and maintained in your Information Security Management Manual (ISMM). Under Part-IS.I.OR.250, the ISMM is a central document that describes

the design, operation, and continual improvement of your ISMS. Operational security processes can be embedded within the ISMM or referenced from it, but in either case, they must be:

- Clearly structured and mapped to aviation-specific risks
- Supported by defined roles and responsibilities
- Linked to evidence logs such as audit trails and incident reports
- Reviewed regularly and updated based on operational changes, audits, or regulatory updates

For each process, define exception scenarios as well - what happens if a flight-critical system is down, or a supplier lacks security evidence. This demonstrates resilience and maturity.

Ongoing management of your ISMM is essential. It must be version-controlled, regularly reviewed, and made available to internal stakeholders and external auditors. The ISMM should evolve with your operations, reflecting real practices rather than static plans.

Finally, once your processes are written and approved, you must implement them and be prepared to demonstrate their effectiveness. This may involve technical deployment, staff training, integration into daily operations, and the collection of performance data. If internal expertise is limited, this is often the stage where bringing in external support can accelerate implementation and ensure compliance is achieved efficiently.

Well-documented, operationalised, and evidenced processes form the practical heart of your ISMS—and are essential to meeting both the letter and the spirit of Part-IS.

Hold Your Management Review Meeting

The Management Review Meeting is a key milestone in formalising your Information Security Management System (ISMS). While it's ideal that these meetings have already been taking place during the ISMS build phase, this first official session marks the point where your system transitions from development into active operation and

governance.

Begin by preparing the meeting environment. Create a dedicated folder to store all relevant meeting records and materials. Use the provided agenda template to build out the meeting structure, and in the section dedicated to “Documents Relevant to Meeting,” list every ISMS-related document - this includes policies, plans, registers, logs, and objectives. Share this list and the document location with the Management Review Team in advance, allowing them time to review materials before the meeting.

During the meeting, walk through each key document, particularly:

- The risk register
- Audit results and findings
- Incident and corrective actions log
- Information security objectives and current performance measures

Include a specific agenda item for formal review and sign-off of ISMS documentation. This is the point where the team collectively confirms that the ISMS is complete, accurate, and ready for use. Seek consensus and document approval for each item.

At the conclusion of the meeting:

- Set all documents to Version 1
- Mark the last review date as the date of the meeting
- Update version control notes to reflect that the document was reviewed and approved during this session

This process may involve a fair amount of administration - updating headers, version tables, and trackers - but it sets a solid baseline for ongoing compliance and audit readiness.

This review represents a major achievement - your ISMS is now considered formally established and aligned with Part-IS requirements. From this point forward, it becomes a living system, managed through ongoing reviews, updates, and improvements.

Communicate Your New Information Security Management System

Once you have signed of and set the baseline version control you are going to publish the documents and communicate to the business that they exist and where they are. Update your communication plan to reflect this.

Operate Your Information Security Management System

In basic terms you will operate the processes you have implemented. You will run your management review meetings, review your measures, conduct your internal audits based on the plan, run your incident management process, run your continual improvement process.

Prepare To Be Audited

As your organisation approaches its first Part-IS audit, it's important to shift from preparation to presentation. At this stage, your ISMS should be fully operational, and now it’s about making sure you’re ready to show it. While audit experiences can vary depending on the individual auditor, preparation and confidence are your best assets.

If you learn the name of your assigned auditor in advance, consider researching their background - for example, via LinkedIn. Their experience often shapes their focus during the audit:

- A background in data protection? Be sure your privacy documentation and processes are rock solid.
- Experience in networking? Double-check your network diagrams, access controls, and system monitoring.
- Software development background? Ensure change control and software assurance processes are airtight.

Regardless of their background, certain fundamentals always matter. Before the audit:

- Ensure all ISMS documents are up to date, version-controlled, and have been reviewed within the last 12 months.
- Reconfirm that all operational processes are functioning as documented.
- Conduct a final internal check - even if you've already completed an internal audit. This is your last chance to catch small issues before they become audit findings.

Educate your team. Those being interviewed or observed during the audit should:

- Answer only what is asked - no extra details that could raise additional questions.
- Be reminded where to find security policies, how to report incidents, and who is responsible for information security in your organisation.

Physically prepare the workspace:

- Ensure employee machines are patched, protected by up-to-date antivirus software, and cleared of clutter (downloads, waste bins, unused files).
- Review admin accounts in key systems. Remove inactive or unnecessary users. Eliminate generic accounts where possible.
- Check physical security practices - enforce clear desk policies, lock away confidential documents, and tidy up print areas and waste bins.

Auditors may also look beyond digital compliance. Common checks include:

- Verifying your cookie policy and checking your website for trackers
- Reviewing your data protection registration (e.g., on the ICO website)
- Checking that fire extinguishers are tested and in date
- Inspecting portable appliance testing (PAT) records for relevant devices

- Examining secure printing areas and confidential waste bins for good housekeeping

Remember, an audit is largely a “show and tell” exercise. Don't give the auditor unnecessary threads to pull - stay focused, structured, and clear in your responses. Reassure your team that the auditor’s role is not to fail you, but to verify your readiness. In most cases, even if non-conformities are found, you’ll be given time to resolve them before certification is impacted.

You're not expected to be perfect - but you are expected to be prepared. If you've followed this roadmap, you're in excellent shape. Take a deep breath, be confident, and remember: you're ready.

Conclusion

You’ve now completed the foundational build of your Information Security Management System (ISMS), aligned with the requirements of Part-IS and tailored specifically to your organisation’s role within the aviation sector. This marks a significant milestone in your journey toward robust, auditable, and sustainable information security management.

At this stage, you have:

- Defined and documented the organisational context, including legal and regulatory obligations
- Assigned clear ownership and accountability for information security tasks
- Developed core policies and operational processes specific to aviation
- Laid the groundwork for a living ISMS that supports both compliance and continual improvement.

Looking ahead, the focus shifts from implementation to ongoing operation. Your efforts will now concentrate on:

- Ensuring processes are followed consistently across the organisation
- Proactively assessing and managing emerging risks

- Conducting regular internal audits and management reviews
- Adapting and updating the ISMS in line with changes to systems, regulations, and operational needs

It's important to remember that Part-IS compliance is not a one-time achievement—- it's a continuous commitment. The strongest ISMS frameworks are those that become part of everyday operations, supported by routine maintenance, active monitoring, and strategic updates.

Should you need support at any stage - whether for audit preparation, policy refinement, technical implementation, or general advice - help is always available. Our Part-IS Implementation toolkit and services are designed to be responsive, practical, and aviation-specific.

By embedding information security into your culture, you're not only fulfilling a regulatory obligation - you're strengthening your organisation's resilience, reputation, and readiness in a fast-evolving sector.

Good Luck. You've got this.