Combination of DOT/FAA AR-08/32 and ISO 14971 processes

*by MSC365 Copilot edited and commented by Peter*

# 1. Integration of the processes

🔹 DOT/FAA AR-08/32 – Requirements Engineering Management

This handbook provides a structured approach to:

* Eliciting, specifying, validating, and managing requirements
* Supporting real-time, embedded systems (e.g., avionics)
* Emphasizing traceability, decomposition, and verification

🔹 ISO 14971 – Risk Management for Medical Devices

This standard defines a lifecycle-based process for:

* Identifying hazards
* Estimating and evaluating risks
* Implementing and verifying risk controls
* Monitoring residual risks and post-market feedback

🔗 Integration Strategy

These two processes complement each other:

|  |  |  |
| --- | --- | --- |
| **ISO 14971** | **DOT/FAA AR-08/32** | **Integration Point** |
| **Define intended use and scope** | Capture system goals and context | Align system boundary and stakeholder needs |
| **Identify hazards and hazardous situations** | Elicit safety-related requirements | Use hazards to derive functional safety requirements |
| **Evaluate risks and define acceptability** | Validate requirements against safety goals | Ensure requirements mitigate unacceptable risks |
| **Design and implement risk controls** | Allocate requirements to architecture | Map risk controls to system/subsystem/component requirements |
| **Verify effectiveness of controls** | Verify requirements and traceability | Use verification artifacts to confirm risk control implementation |
| **Monitor post-production risks** | Manage requirements changes | Feed operational data into requirement updates |

🧭 Notes on Integration

* **ISO 14971** provides the **risk-driven rationale** for safety requirements.
* **FAA AR-08/32** ensures those requirements are **well-specified, allocated, and verified**.
* The combined process supports **model-based development**, **traceability**, and **formal assurance**.

# 2. Combined process outline

**Remark**: *This outline and the detailed description (Ch. 4) are different in some steps, e.g.,*

* *Safety objectives are established in step 8 in the outline while in Step 3 in the detailed description*
* *Some steps are combined Outline 2&3 ~ Detailed 2*
* *Additional step: Detailed 11*
* *Abandoned step: Outline Step 20*
* *Some steps are slightly differently named, some are more different like Outline 17 vs. Detailed 17*

Phase 1: Planning & Scoping

1. **Define Intended Use** (ISO 14971)
2. **Establish System Goals and Context** (FAA AR-08/32)
3. **Identify Stakeholders and Operational Environment**

Phase 2: Hazard & Risk Analysis

1. **Identify Hazards and Hazardous Situations** (ISO 14971)
2. **Estimate Risk (Severity × Probability)**
3. **Evaluate Risk Acceptability**
4. **Document Risk Management Plan and Criteria**

Phase 3: Requirements Derivation

1. **Define Safety Objectives** (from risk analysis)
2. **Derive Risk Control Functional Requirements**
3. **Capture System-Level Requirements** (FAA AR-08/32)
4. **Validate Requirements Against Safety Goals**

Phase 4: Architecture & Allocation

1. **Define System Architecture**
2. **Allocate Requirements to Subsystems and Components**
3. **Ensure Traceability from Risk Controls to Requirements**

Phase 5: Verification & Validation

1. **Verify Requirements Implementation**
2. **Validate Risk Control Effectiveness**
3. **Document Evidence in Risk Management File and Requirements Baseline**

Phase 6: Maintenance & Monitoring

1. **Monitor Residual Risk and Operational Feedback**
2. **Update Requirements and Risk Controls as Needed**
3. **Maintain Traceability and Change History**

# 3. Abandoned or modified steps from DOT/FAA AR-08/32 and ISO 14971 in the combined process

✅ Steps Retained and Integrated

From ISO 14971:

* **Intended Use Definition**
* **Hazard Identification**
* **Risk Estimation and Evaluation**
* **Risk Control Identification and Implementation**
* **Residual Risk Evaluation**
* **Risk Control Verification**

These are retained because they directly inform the derivation of **safety-related requirements**, which are then managed through the FAA-style requirements process.

From FAA AR-08/32:

* **Requirements Elicitation and Analysis**
* **Requirements Specification**
* **Requirements Validation**
* **Requirements Allocation**
* **Traceability and Change Management**

These are essential for ensuring that the risk-derived requirements are **well-formed, allocated, and verifiable**.

❌ Steps Abandoned or Significantly Modified

🔻 From ISO 14971:

|  |  |
| --- | --- |
| **Step** | **Reason for Abandonment/Modification** |
| **Production and Post-Production Monitoring** | In the FAA context, especially for early design or illustrative examples like Isolette, post-market surveillance is often out of scope. Instead, the focus is on design-time assurance. |
| **Risk-Benefit Analysis** | FAA AR-08/32 does not emphasize benefit-risk trade-offs in the same way. In safety-critical domains like aviation, risk acceptability is often absolute, not relative. |

🔻 From FAA AR-08/32:

|  |  |
| --- | --- |
| **Step** | **Reason for Abandonment/Modification** |
| **Use of Informal Scenarios for Requirements Discovery** | ISO 14971 requires structured hazard analysis. Informal use cases are replaced or supplemented by hazard-driven scenarios. |
| **Requirements Prioritization Based on Stakeholder Value** | In safety-critical systems, risk severity and likelihood take precedence over stakeholder preference. Prioritization is risk-driven, not value-driven. |
| **Generic Requirements Templates** | These may be too vague for safety-critical risk controls. ISO 14971 demands specific, testable mitigations. Templates are replaced with risk-informed requirement patterns. |

Prompt [Make a more detailed description of the combined process. Also include information for each step origin w.r.t. ISO 14971 or FAA AR-08/32.](https://m365.cloud.microsoft/chat/entity1-d870f6cd-4aa5-4d42-9626-ab690c041429/eyJpZCI6IlZYTmxjbFl4ZkdoMGRIQnpPaTh2YzNWaWMzUnlZWFJsTFdsdWRDNXZabVpwWTJVdVkyOXRMM3hQU1VRNk9XUmlOMlJsTXpZdE4yVmxaUzAwWTJJNExUazNOelF0T0RnMk56TmtZV0V6WVdaa2ZETTFNVEZsT0dWaUxUQXdaVGd0TkdVek5TMDVNak16TFdNME9XTXdOakZqTldaaVpId3lNREkxTFRBM0xUSXpWREU1T2pRMk9qVTJMamN6T1RVMU1EbGEiLCJzY2VuYXJpbyI6InNoYXJlTGlua1ZpYVBhZ2UiLCJwcm9wZXJ0aWVzIjp7InByb21wdFNvdXJjZSI6InVzZXIiLCJjbGlja1RpbWVzdGFtcCI6IjIwMjUtMDctMjNUMTk6NDY6NTcuMzY0WiJ9LCJjaGF0VHlwZSI6IndlYiIsInZlcnNpb24iOjEuMX0)

Here’s a **detailed description** of a **combined process** that integrates the **DOT/FAA AR-08/32 Requirements Engineering Management** and the **ISO 14971 Risk Management** process, with each step annotated by its origin.

# 4. Combined Process: From Concept to Component-Level Safety Requirements

## Phase 1: Planning and Scoping

|  |  |  |
| --- | --- | --- |
| **Step** | **Description** | **Origin** |
| **1. Define Intended Use and Scope** | Establish the purpose, operational context, and boundaries of the system. | ISO 14971 |
| **2. Identify Stakeholders and System Context** | Capture stakeholder needs, operational scenarios, and environmental assumptions. | FAA AR-08/32 |
| **3. Establish Safety Objectives** | Define high-level safety goals based on intended use and potential harms. | ISO 14971 |

## Phase 2: Hazard and Risk Analysis

|  |  |  |
| --- | --- | --- |
| **Step** | **Description** | **Origin** |
| **4. Identify Hazards and Hazardous Situations** | Analyze potential sources of harm and their contexts. | ISO 14971 |
| **5. Estimate Risk (Severity × Probability)** | Quantify risk levels for each hazardous situation. | ISO 14971 |
| **6. Evaluate Risk Acceptability** | Determine which risks require mitigation. | ISO 14971 |
| **7. Document Risk Management Plan** | Define criteria, responsibilities, and traceability for risk control. | ISO 14971 |

## Phase 3: Requirements Derivation and Specification

|  |  |  |
| --- | --- | --- |
| **Step** | **Description** | **Origin** |
| **8. Derive Risk Control Functional Requirements** | Translate risk controls into functional requirements. | ISO 14971 |
| **9. Capture System-Level Requirements** | Specify all system functions, including safety-related ones. | FAA AR-08/32 |
| **10. Validate Requirements Against Safety Objectives** | Ensure requirements address identified risks and stakeholder needs. | FAA AR-08/32 |
| **11. Classify Requirements (Safety vs. Non-Safety)** | Distinguish safety-critical requirements from others. | ISO 14971 + FAA AR-08/32 |

## Phase 4: Architecture and Allocation

|  |  |  |
| --- | --- | --- |
| **Step** | **Description** | **Origin** |
| **12. Define System Architecture** | Identify subsystems, components, and interfaces. | FAA AR-08/32 |
| **13. Allocate Requirements to Subsystems and Components** | Map functional and safety requirements to architectural elements. | FAA AR-08/32 |
| **14. Ensure Traceability from Risk Controls to Components** | Maintain linkage from hazards to component-level mitigations. | ISO 14971 + FAA AR-08/32 |

## Phase 5: Verification and Validation

|  |  |  |
| --- | --- | --- |
| **Step** | **Description** | **Origin** |
| **15. Verify Requirements Implementation** | Confirm that design meets specified requirements. | FAA AR-08/32 |
| **16. Validate Risk Control Effectiveness** | Demonstrate that risk controls reduce risk to acceptable levels. | ISO 14971 |
| **17. Document Evidence and Traceability** | Maintain records of verification, validation, and risk control implementation. | ISO 14971 + FAA AR-08/32 |

## Phase 6: Maintenance and Monitoring (Optional in design-time assurance)

|  |  |  |  |
| --- | --- | --- | --- |
| **Step** | **Description** | **Origin** | **Status** |
| **18. Monitor Residual Risk and Operational Feedback** | Post-market surveillance and feedback loop. | ISO 14971 | Often excluded in design-time assurance |
| **19. Update Requirements and Risk Controls** | Reflect changes based on operational data. | ISO 14971 | Optional |