Memorandum

U.S. Department
of Transportation

Federal Railroad
Administration

Date: APR - 1 2014

Subject: Positive Train Control Technical Bulletin PTC-14-01
Positive Train Control: Safety Plan (PTCSP) Review Guidance

From: Robert C. Lauby Robert C Lauby
Associate Administrator for Railroad Safety
Chief Safety Officer

To: All Federal Railroad Administration Staff Directors, Field Employees, and
Participating State Employees

The purpose of this technical bulletin is to provide the Federal Railroad Administration (FRA) Office of Railroad Safety personnel with guidance regarding the appropriate minimum level of Positive Train Control Safety Plan (PTCSP) reviews required in support of Positive Train Control (PTC) system certification required by the Rail Safety Improvement Act of 2008 (RSIA).

Certification of PTC systems is required by 49 U.S.C. § 20157(h). This statute states that "The Secretary shall not permit the installation of any positive train control system or component in revenue service unless the Secretary has certified that any such system or component has been approved through the approval process set forth in part 236 of title 49, Code of Federal Regulations, and complies with the requirements of that part."

A critical element of PTC system certification is that FRA can reasonably determine if a railroad's engineering and test efforts demonstrate that the PTC system implements the following required core functions while trains are operating seamlessly across and between different railroads:

- Reliably and functionally prevent train-to-train collisions.
- Reliably and functionally prevent overspeed derailments.
- Reliably and functionally prevent incursions into established work zone limits without first receiving appropriate authority and verification from the dispatcher or roadway worker in charge, as applicable.
- Reliably and functionally prevent the movement of a train through a mainline switch in the improper position.

The PTCSP is the document that (1) presents the case that the system in question satisfies the preceding criteria, and (2) presents the safety argument that the system satisfies the appropriate requirement of Title 49 Code of Federal Regulations (CFR) Section 236.1015(e) for non-vital overlay, vital overlay, standalone, and mixed PTC systems.

The implementing regulations for 49 U.S.C. § 20157 are found in 49 CFR Part 236, Subpart I. These regulations are performance based. Although performance-based regulations give a high degree of latitude to both the regulator and the regulated entity, the extent of compliance often can be highly subjective. Compliance with the guidance outlined in the attachment (Positive Train Control: Safety Plan Review Guidance, Version 1.0) will reduce that subjectivity and provide greater uniformity to the review process.

Questions should be directed to Dr. Mark Hartong, Senior Scientific/Technical Advisor, at (202) 493-1332 or Mark.Hartong@dot.gov.

Attachment

Version 1.0

U.S. Department of Transportation
Federal Railroad Administration

POSITIVE TRAIN CONTROL: SAFETY PLAN REVIEW GUIDANCE

Office of Railroad Safety
Washington, DC 20590

FOREWORD

This document provides guidance for FRA personnel reviewing Positive Train Control (PTC) Safety Plans (PTCSP) prior to system certification. It augments the following field audit guidance documents: "General Monitoring and Audit Guidelines: Positive Train Control Systems," "Field Audit Checklist: Positive Train Control Systems Functional Testing Process," "Braking Test Model Extrapolation Positive Train Control Systems," and "Field Audit Checklist: Positive Train Control Systems Track Database Implementation Process." It presumes that the testing for the PTC system being considered for certification has been successfully completed, and audited with no outstanding negative findings.

The Office of Railroad Safety guidelines in this document ensure an appropriate minimum level of PTCSP review required in support of PTC system certification required by the Rail Safety Improvement Act of 2008 (RSIA). Since it is impractical to cover all situations or conditions that may arise, the auditor or monitor must supplement them with good judgment as required.

Please forward any deficiencies, clarifications, or suggested improvements regarding the content of this document to the Signal and Train Control Division Staff Director, Federal Railroad Administration, 1200 New Jersey Avenue SE, Washington, DC 20590.

Table of Revisions

Version	Date	Notes
1.0	3/19/14	Technical bulletin routed for issuance

TABLE OF CONTENTS

Introduction

Background

Certification of PTC systems is required by 49 U.S.C. § 20157(h). This statute states that "The Secretary shall not permit the installation of any positive train control system or component in revenue service unless the Secretary has certified that any such system or component has been approved through the approval process set forth in part 236 of title 49, Code of Federal Regulations, and complies with the requirements of that part."

A critical element of PTC system certification is that the Federal Railroad Administration (FRA) can reasonably determine if a railroad's engineering and test efforts demonstrate that the PTC system implements the required core functions:

- Reliably and functionally prevent train-to-train collisions.
- Reliably and functionally prevent overspeed derailments.
- Reliably and functionally prevent incursions into established work zone limits without first receiving appropriate authority and verification from the dispatcher or roadway worker in charge, as applicable.
- Reliably and functionally prevent the movement of a train through a mainline switch in the improper position.
- All while trains are operating seamlessly across and between different railroads.

The PTCSP is the document that (1) presents the case that the system in question satisfies the preceding criteria, and (2) presents the safety argument that the system satisfies the appropriate requirement of Title 49 Code of Federal Regulations (CFR) Section 236.1015(e) for nonvital overlay, vital overlay, standalone, and mixed PTC systems.

The implementing regulations for 49 U.S.C. § 20157 are found in 49 CFR Part 236, Subpart I. These regulations are performance based. Although performance-based regulations give a high degree of latitude to both the regulator and the regulated entity, the extent of compliance often can be highly subjective. Compliance with the requirements of this document should reduce that subjectivity, and provide greater uniformity of the review process. Even with the guidelines in this document, each review will vary slightly, depending on the individual railroad property, the PTC system they chose to implement, their approach to system safety, and their demonstration of compliance with the plans and process they specify.

This document is not a substitute for good judgment, experience, and common sense.

As is the case with other regulatory requirements, responsibility for compliance is with the railroads. The railroad retains ultimate responsibility not only for their actions, but also for the actions of their contractors and subcontractors.

Review Duration

PTCSPs undergo three levels of review at FRA. First, is the initial technical review to determine if the package submitted by the railroad meets a minimum level of technical adequacy and has the required content to warrant further detailed technical review and analysis by subject matter experts. Second, is a detailed technical review and analysis by subject matter experts to determine the technical adequacy of the contents of the PTCSP. The third review is management oversight review for consistency.

It is important to note that while FRA has established a target of 180 days for the review and approval of the PTCSP (See 49 CFR § 236.1009(j)(2)(ii)), in any situation where artificial compliance with a schedule threatens to compromise the technical integrity of any review, FRA will extend the review period as necessary. FRA will provide an explanation of the delay, a new projected deadline, and identify any additional information that may be required. (See 49 CFR § 236.1009(j)(2)(iii)). Given the administrative lead times, the FRA technical lead must initiate this notification process no later than at Day 120 to ensure the notification is ready by Day 180.

Intellectual Property and Proprietary Information

The PTCSP will often contain valuable intellectual property and or proprietary information. Intellectual property refers to valuable intangible property created by the human mind. It includes items such as:

- Patents: A grant of a property right by the Government to an inventor that allows the inventor "to exclude others from making, using, or selling the invention."
- Copyrights: A form of protection provided by U.S. law to authors of "original works or authorship" fixed in any tangible medium of expression.
- Trademarks: Anything used in the marketplace to distinguish goods or services of one source from those of other sources. Typically, it is a word or symbol, but it can also be other things.

Much intellectual property is available to the public; however, such availability does not give the public authorization to use the information without compensation to the owner of the information.

Proprietary information, on the other hand, is for the sole knowledge of its owners, and is normally not available outside the business. This includes details such as company financials, tax compliance, client financials, customer lists, and pricing information, as well as trade secrets, such as research and development, formulas, and software programs. Obtaining proprietary information by competitors can provide them with valuable intelligence, for example, by knowing what bid package is being put together by the entrepreneur for winning a contract.

Misuse of Proprietary and Trade Secret Information

There are severe legal penalties for the mishandling of proprietary and trade secret information.

The Economic Espionage Act contains two separate provisions that make the theft or misappropriation of trade secrets a Federal criminal offense. The first provision, under Section 1831, is directed toward foreign economic espionage and requires that the theft of a trade secret be done to benefit a foreign government, instrumentality, or agent. In contrast, the second provision, under Section 1832, makes the commercial theft of trade secrets a criminal act regardless of who benefits.

A defendant convicted of economic espionage under Section 1831 can be imprisoned for up to 15 years and fined $500,000 or both. Corporations and other organizations can be fined up to $10 million. A defendant convicted of the theft of trade secrets under Section 1832 can be imprisoned for up to 10 years and fined $500,000 or both. Corporations and other entities can be fined no more than $5 million.

Three other laws apply to disclosure of specific types of proprietary information, especially disclosure by government personnel:

- For knowing disclosure of nongovernment information to which a Government agency has gained access in connection with a procurement action, 41 U.S.C. 423, Procurement Integrity, provides both civil and criminal penalties. The criminal penalty is up to 5 years imprisonment. The civil penalty is a fine up to $100,000. This applies mainly to Government employees who receive nongovernment information, but also to nongovernment personnel who receive sensitive procurement information from the Government (for example, if the Government gives an industry representative a bid package containing information from a potential subcontractor). This procurement integrity law applies only prior to the award of a contract. Once a contract has been awarded, other laws with lesser penalties may apply.

- Title 18 U.S.C. 1905 applies to disclosure by a Government employee of any information provided to the Government by a company or other nongovernment organization, if the provider of the information identified it as proprietary or as being provided to the Government in confidence. The penalty is mandatory removal from office (termination of employment), and the offender may be fined no more than $1,000 and imprisoned no more than 1 year.

- For disclosure of nongovernment financial information in the custody of the Government, civil remedies are allowed under 12 U.S.C. 417, Civil Penalties, which also requires the director of the Office of Personnel Management (OPM) to conduct an investigation and recommend disciplinary action on Federal employees found culpable.

Requests for Confidentiality

Entities wishing to claim confidentiality for any information submitted to FRA must abide by the requirements of 49 CFR § 209.11. This places very specific requirements on the submitting entity. Entities wishing to request confidentiality for material must be referred to the FRA Office of Chief Counsel. They should also be told that:

- Any document containing information for which confidential treatment is requested shall be accompanied at the time of filing by a statement justifying nondisclosure and referring to the specific legal authority claimed.

- Any document containing any information for which confidential treatment is requested shall be marked "CONFIDENTIAL" or "CONTAINS CONFIDENTIAL INFORMATION" in bold letters. If confidentiality is requested for the entire document, or if it is claimed that nonconfidential information in the document is not reasonably able to be separated from the confidential information, the accompanying statement of justification shall so indicate. If confidentiality is requested for a portion of the document, then the person filing the document shall file together with the document a second copy of the document from which the information for which confidential treatment is requested has been deleted. If the person filing a document of which only a portion is requested to be held in confidence does not submit a second copy of the document with the confidential information deleted. FRA may assume that there is no objection to public disclosure of the document in its entirety.

- FRA retains the right to make its own determination with regard to any claim of confidentiality. Notice of a decision by FRA to deny a claim, in whole or in part, and an opportunity to respond shall be given to a person claiming confidentiality of information no less than 5 days prior to its public disclosure.

Initial Technical Review

The primary purpose of initial document review is to review the submitted PTCSP and determine whether the railroad is responsive or nonresponsive, as it pertains to the regulatory requirements.

The minimum regulatory content for the PTCSP is derived directly from 49 CFR § 236.1015 and listed in the "Initial Review Checklist." As part of the initial review process, the reviewer must ensure that the PTCSP addresses this information either directly, or through incorporation by reference of an appropriate PTC Development Plan (PTCDP) Type Approval.

The initial review is not required to determine if any of these are items are technically correct, only that they are present. Subsequent detailed reviews by the various subject matter experts will make the determination if they are technically correct. The initial determination is simply to estimate if there is there is sufficient information present to begin a detailed analysis. If insufficient information is available, which would be indicted by "N" or "No" in the information present column of the checklist, the railroad will be formally notified in writing of the missing information necessary required to resume the evaluation process.

Required Information Attribute	**Information Present (Y/N)**
A complete description of the PTC system, including a list of all PTC system components and their physical relationships in the system or subsystem.	
A description of the railroad operation or categories of operations on which the PTC system is designed to be used, including train movement density (passenger, freight), operating speeds (including a thorough explanation of intended compliance with additional requirements for high-speed service), track characteristics, and railroad operating rules.	
An operational concepts document, including a list with complete descriptions of all functions that the PTC system will perform to enhance or preserve safety.	
A document describing the manner in which the PTC system architecture satisfies safety requirements.	
A preliminary human factors analysis, including a complete description of all human-machine interfaces and the impact of interoperability requirements on the same.	
An analysis of the applicability to the PTC system of the requirements of Subparts A through G that may no longer apply or are satisfied by the PTC system using an alternative method, and a complete explanation of the manner in which those requirements are otherwise fulfilled.	
A prioritized service restoration and mitigation plan, and a description of the necessary security measures for the system.	
A description of target safety levels (e.g., MTTHE for major subsystems as defined in Subpart H), including requirements for system availability and a description of all backup methods of operation and any critical assumptions associated with the target levels.	
A complete description of how the PTC system will enforce authorities and signal indications.	
A complete description of how the PTC system will appropriately and timely enforce all integrated hazard detectors if applicable.	

A hazard log consisting of a comprehensive description of all safety-relevant hazards not previously addressed by the vendor or supplier to be addressed during the life cycle of the PTC system, including maximum threshold limits for each hazard (for unidentified hazards, the threshold shall be exceeded at one occurrence).	
A description of the safety assurance concepts that are to be used for system development, including an explanation of the design principles and assumptions.	
A risk assessment of the as-built PTC system described.	
A hazard mitigation analysis, including a complete and comprehensive description of each hazard and the mitigation techniques used.	
A complete description of the safety assessment and verification and validation processes applied to the PTC system, their results, and whether these processes address the safety principles described in Appendix C directly, using other safety criteria, or not at all.	
A complete description of the railroad's training plan for railroad and contractor employees and supervisors necessary to ensure safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the PTC system.	
A complete description of the specific procedures and test equipment necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the PTC system on the railroad and establish safety-critical hazards are appropriately mitigated. These procedures, including calibration requirements, shall be consistent with or explain deviations from the equipment manufacturer's recommendations.	
A complete description of any additional warning to be placed in the Operations and Maintenance Manual and all warning labels to be placed on equipment as necessary to ensure safety.	
A complete description of the configuration or revision control measures designed to ensure that the railroad or its contractor does not adversely affect the safety-functional requirements and that safety-critical hazard mitigation processes are not compromised as a result of any such change.	
A complete description of all initial implementation testing procedures necessary to establish that safety-functional requirements are met and safety-critical hazards are appropriately mitigated.	

A complete description of all post-implementation testing (validation) and monitoring procedures, including the intervals necessary to establish that safety-functional requirements, safety-critical hazard mitigation processes, and safety-critical tolerances are not compromised over time, through use, or after maintenance (adjustment, repair, or replacement) is performed.	
A complete description of each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, tests, adjustments, repairs, or replacements, and the system's resulting conditions, including records of component failures resulting in safety-relevant hazards.	
A safety analysis to determine whether (when the system is in operation) any risk remains of an unintended incursion into a roadway work zone due to human error. If the analysis reveals any such risk, the PTCDP and PTCSP shall describe how that risk will be mitigated.	
A complete description of how the PTC system will enforce authorities and signal indications, unless already completely provided for in the PTCDP.	
A description of how the PTCSP complies with 49 CFR § 236.1019(f), if applicable;	
A description of any deviation in operational requirements for en route failures as specified under 49 CFR § 236.1029(c), if applicable and unless already completely provided for in the PTCDP.	
A complete description of how the PTC system will appropriately and timely enforce all integrated hazard detectors in accordance with 49 CFR § 236.1005.	
An emergency and planned maintenance temporary rerouting plan indicating how operations on the subject PTC system will take advantage of the benefits provided under 49 CFR § 236.1005(g) through (k).	
The documents and information required under additional requirements for high-speed service and communications and security requirements.	

Requirements Review

The detailed technical review for the PTCSP is significantly more complex, and lends itself to a much more subjective evaluation than the initial review. When conducting the detailed technical review, the reviewer must continually ask themselves (1) if the requirements are technically correct and coherent, and (2) does the information provided support a plausible explanation that justifies any claims made.

Requirement Clarity

Required Information Attribute	**Information Present (Y/N)**
Are the requirements written in nontechnical understandable language?	
Are there any requirements, which could have more than one interpretation?	
Is each characteristic of the final product described with a unique terminology?	
Is there a glossary in which the specific meanings of each term are defined?	
Could the requirements be understood and implemented by an independent group?	

Requirement Completeness

Required Information Attribute	**Information Present (Y/N)**
Are all figures, tables, and diagrams labeled?	
Are all figures, tables, and diagrams cross-referenced?	
Are all terms defined?	
Are all terms indexed?	
Are all units of measure defined?	
Are areas where information is incomplete because development has not started been specified?	
Is the missing information defined in the requirement?	
Should any requirement be specified in more detail?	
Should any requirement be specified in less detail?	
Are all of the requirements defined?	
Are all of the requirements related to functionality included?	
Are there any requirements that make you feel uneasy?	
Are all of the requirements related to performance included?	
Are all of the requirements related to design constraints included?	
Are all of the requirements related to attributes included?	
Are all of the requirements related to external interfaces included?	
Are all of the requirements related to databases included?	
Are all of the requirements related to software included?	
Are all of the requirements related to communications included?	
Are all of the requirements related to hardware included?	
Are all of the requirements related to inputs included?	
Are all of the requirements related to outputs included?	

Required Information Attribute	Information Present (Y/N)
Are all of the requirements related to reporting included?	
Are all of the requirements related to security included?	
Are all of the requirements related to maintainability included?	
Are all of the requirements related to installation included?	
Are all of the requirements related to criticality included?	
Are all of the requirements related to the permanency limitations included?	
Are possible changes to the requirements specified?	
Is the likelihood of change specified for each requirement?	

Requirement Consistency

Required Information Attribute	Information Present (Y/N)
Are there any requirements describing the same object that conflict with other requirements with respect to terminology?	
Are there any requirements describing the same object that conflict with respect to characteristics?	
Are there any requirements that describe two or more actions that conflict logically?	
Are there any requirements that describe two or more actions that conflict temporally?	

Requirement Traceability

Required Information Attribute	Information Present (Y/N)
Are all requirements traceable back to a specific user need?	
Are all requirements traceable back to a specific source document or person?	
Are all requirements traceable forward to a specific design document?	
Are all requirements traceable forward to a specific software module?	

Requirement Verifiability

Required Information Attribute	Information Present (Y/N)
Are any requirements included that are impossible to implement?	
For each requirement, is there a process that can be executed by either a human or a machine to verify the requirement?	

Required Information Attribute	Information Present (Y/N)
Are there any requirements that will be expressed in verifiable terms at a later time?	

Requirement Modifiability

Required Information Attribute	Information Present (Y/N)
Is the requirement document clearly and logically organized?	
Does the organization adhere to an accepted standard?	
Is there any redundancy in the requirements?	

Requirement Content

Required Information Attribute	Information Present (Y/N)
Is each requirement relevant to the problem and its solution?	
Are any of the defined requirements really design details?	
Are any of the defined requirements really verification details?	
Are any of the defined requirements really project management details?	
Is there an introduction section?	
Is there a general description section?	
Is there a scope section?	
Is there a definitions, acronyms, and abbreviations section?	
Is there a specific requirements section?	
Is there a product perspective section?	
Is there a product functions section?	
Is there a user characteristics section?	
Is there a general constraints section?	
Is there an assumptions and dependencies section?	
Is there a specific requirements section?	
Are all of the necessary appendices present?	
Are all of the necessary figures present?	
Are all of the necessary tables present?	
Are all of the necessary diagrams present?	
Are all input sources specified?	
Are all input accuracy requirements specified?	
Are all input range values specified?	
Are all input frequencies specified?	
Are all input formats specified?	
Are all output destinations specified?	
Are all output accuracy requirements specified?	

Required Information Attribute	**Information Present (Y/N)**
Are all output range values specified?	
Are all output frequencies specified?	
Are all output formats specified?	

Functionality Review

System Functionality

Required Information Attribute	**Information Present (Y/N)**
Are all software functions specified?	
Are all inputs specified for each function?	
Are all aspects of the processing specified for each function?	
Are all outputs specified for each function?	
Are all performance requirements specified for each function?	
Are all design constrains specified for each function?	
Are all attributes specified for each function?	
Are all security requirements specified for each function?	
Are all maintainability requirements specified for each function?	
Are all database requirements specified for each function?	
Are all operational requirements specified for each function?	
Are all installation requirements specified for each function?	

System External Interfaces

Required Information Attribute	**Information Present (Y/N)**
Are all user interfaces specified?	
Are all batch interfaces specified?	
Are all hardware interfaces specified?	
Are all software interfaces specified?	
Are all communications interfaces specified?	
Are all interface design constraints specified?	
Are all interface security requirements specified?	
Are all interface maintainability requirements specified?	
Are all human-computer interactions specified for user interfaces?	

System Internal Interfaces

Required Information Attribute	Information Present (Y/N)
Have all internal interfaces been identified?	
Have all internal interfaces characteristics been specified?	
Are all expected processing times specified?	
Are all data transfer rates specified?	
Are all system throughput rates specified?	
Are the consequences of software failure specified for each requirement?	
Is the information to protect from failure specified?	
Is a strategy for error detection specified?	
Is a strategy for correction specified?	
Are acceptable trade-offs specified for competing attributes?	

System Hardware

Required Information Attribute	Information Present (Y/N)
Is the minimum memory specified?	
Is the minimum storage specified?	
Is the maximum memory specified?	
Is the maximum storage specified?	

System Software

Required Information Attribute	Information Present (Y/N)
Are the required software environments/operating systems specified?	
Are all of the required software utilities specified?	
Are all purchased software products that are to be used with the system specified?	

System Communications

Required Information Attribute	Information Present (Y/N)
Is the target network specified?	
Are the required network protocols specified?	
Is the required network capacity specified?	
Is the required/estimated network throughput rate specified?	
Is the estimated number of network connections specified?	
Are minimum network performance requirements specified?	

Required Information Attribute	Information Present (Y/N)
Are the maximum network performance requirements specified?	
Are the optimal network performance requirements specified?	

Risk Assessment Review

The following is a list of items to consider when reviewing the adequacy of the Risk Assessment of the PTCSP:

Process and Planning

Required Information Attribute	Information Present (Y/N)
Is each product or program developed under a continuous risk management process?	
Is risk management required as a part of the normal business of program/project meetings? (This is preferred as opposed to risk management conducted in special, splinter meetings.)	
Are records of program/project meeting minutes showing what risk management activities were conducted and when required as auditable records?	
Is proof of qualified adequate resources required to be applied to the risk management effort?	
How are risks identified?	
Is the identification process effective?	

Hazard Identification

Required Information Attribute	Information Present (Y/N)
Does each product or program developed require the risk management process to begin during conceptual design prior to the preliminary design beginning with a preliminary hazard analysis?	
Does the risk management process require adequate specification that:	
• Identified hazards must be eliminated or controlled?	
• Hazards including discrepancies and corrective actions must be recorded for risk management purposes?	

• The approach for implementing this requirement is documented?	
Does the risk management process require adequate discussion of appropriate hazard controls? Does this include:	
• Approach to consideration and selection of controls?	
• Use of hazard reduction precedence sequences?	
• Approach to identifying and accepting any residual risk?	
• Implementation of controls including verifying effectiveness?	
• Scope of coverage (hazardous chemicals, equipment, discharges, waste, energies, etc.)	
Does the risk management process require adequate discussion of hazardous operations? Does this include:	
• Methods for notification of personnel when hazardous operations are to be performed or when hazardous conditions are found to exist?	
• Methods for defining, classifying, and prioritizing hazardous operations?	
• Methods for developing and defining a list of hazardous operations?	
• Methods for identifying, developing, reviewing, approving, and making readily available written hazardous operations procedures with particular emphasis on identifying the job safety steps required?	
• Methods for addressing management of hazardous materials and wastes?	

Hazard Analysis

Required Information Attribute	**Information Present (Y/N)**
How are risks analyzed? For example, does the does the risk analysis use Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA), or Probabilistic Risk Assessment (PRA)?	
How is the effectiveness of the analysis process evaluated?	
Has each risk required been assessed and quantified as to probability and consequences (including cost consequences)?	
How are risks prioritized?	
How and when are risks updated when a change in program phase occurs, or when significant changes in program scope, budget, or schedule occur?	
Has responsibility to address each risk been assigned to a person?	

Hazard Mitigation

Required Information Attribute	Information Present (Y/N)
Have mitigation plans been required to be prepared and implemented and responsibility assigned?	
How is it determined that adequate resources have been assigned for effective implementation of the risk mitigation plans?	
How are risks and risk trends tracked?	
Is the risk tracking method effective?	
How are all mitigated and monitored risks being regularly tracked to ascertain trends and ensure that trigger levels are not being exceeded?	
How is acceptance of identified risks of a product by appropriate level of management obtained and recorded? Are all risk acceptances documented?	
What risks are required to be disposed of prior to delivery and operation?	
How is access to the risk list specified?	
Are risks regularly required to be presented by the developer to the customer?	
Is a database system used as a tool to provide current, up-to-date information to all involved parties?	

System Reports

Required Information Attribute	Information Present (Y/N)
Are all report formats specified?	
Are all calculations/formulas used in reports specified?	
Are all report data filter requirements specified?	
Are all report sorting requirements specified?	
Are all report totaling requirements specified?	
Are all report formatting requirements specified?	

Final Management Review

The management oversight review results in the formal approval and certification of a system. This review considers the results of the detailed technical review, the original petition contents, and any additional developed facts to render a final decision. The following items must be addressed in the final review:

1. The purpose of the document is clear and understood by the audience expected to use the document.

2. The document format adheres to the approved methodology for the project.

3. The audience is knowledgeable of the intent and content of those standards.

4. Material content is traceable. Traceability is clear and conforms to acceptable standards.

5. Information is presented with the terminology and level of detail appropriate to the audience and intent of the document.

6. Information content provides clear and unambiguous descriptions. The level of detail provided in the description of the component is sufficient to ensure consistent interpretation.

7. Each requirement, directive, or key data component is explicitly verifiable. Requirements must be complete and not open to interpretation; tasks must reflect measurable statements; design statements must correlate to specific requirements.

8. Document review indicates inclusion of all critical information and reflects a thorough analysis of the situation.

9. Statements made in one section of the document do not conflict with statements made in other areas of document.

10. Document contents are presented in a meaningful and organized fashion enabling effective use of the information in the execution of related tasks; for example, requirements specifications directly linking to test matrices.

11. The document is evidenced to be in use as it was originally proposed (i.e. requirements directing design activities, high level design directing detail design, strategic test plan directing detail test planning activities).

12. The document effectively enables updates to occur. Document change processes are included in the description. Version control is maintained over the document.

13. Approval processes and review schedules are included in the release of the document. Planned revisions are scheduled.

14. Summary background and orientation directly support the creation of detail design specifications.

15. Format of the document is clear and readily enables the reader to understand the relationship between business needs, safety needs, and the design to fulfill them.

16. Format is defined or intuitively clear—not a random flow of information, but an orchestrated set of specifications.

17. Summary of business needs are provided.

18. Summary of changes in context to the current system is provided.

19. Design elements are directly traceable to documentation requirements and documentation requirements are traceable to design statements.

20. Tracing requirements adhere to naming convention.

21. Tracing requirements include static and dynamic processes. Design statements accurately and thoroughly comply with intentions indicated in requirements.

22. A consistent level of detail is provided within the design statement.

23. The design components, functional processes, usability, ease of maintenance, portability, performance, tolerance and reliability, access authorization, integrity, and systems interfaces conform to stated requirements. Critical categories are:
    a. Clear and unambiguous.
    b. Defined in a thorough and complete fashion.
    c. Explicitly verifiable.
    d. Conflict free.
    e. Provided in a presentable format.
    f. Identified in requirements.