



GUIDANCE NOTES ON

SOFTWARE PROVIDER CONFORMITY PROGRAM

ABS CyberSafety™ VOLUME 5

SEPTEMBER 2016

**American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862**

**© 2016 American Bureau of Shipping. All rights reserved.
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA**

Foreword

The importance of the development of a positive safety culture has been recognized for some time, particularly in large-scale systems where the consequences of losses may be severe. The marine and offshore industries are increasingly reliant on computer-based control systems; therefore, the specification and verification of the software used in the control systems and their integration into the system is an important element of safety assessments. This document has been developed with the objective of improving safety and environmental performance of ships and offshore assets by providing a process to improve control system software quality. The American Bureau of Shipping (ABS) provides this guidance in recognition of the beneficial effect that high software quality installed in various control systems has on the performance of assets.

The *ABS Guide for Integrated Software Quality Management (ISQM)* presents a risk-based software development and maintenance process for application on ships and offshore assets that is based upon internationally recognized standards. These Guidance Notes augment the *ISQM Guide* by documenting procedures and recommendations developed with input from ABS clients and software development professionals and best practices for quality software development. The guidance provided is based on industry-accepted software quality development activities and practices that are applicable to software System Providers (SPs) who are internally implementing and evaluating their application of ABS' ISQM processes. The Guidance Notes are also intended to help providers of control system software gain recognition of their quality software development policies, procedures, and practices. The guidance is applicable to all divisions, groups, and companies engaged in developing, supplying, deploying, and maintaining software, and provides information to assist SPs in preparing for ABS' ISQM conformity assessments.

The information in this document is sufficiently general to allow SPs appropriate latitude in software development practices, yet sufficiently detailed so as to provide useful guidance to SPs as they implement an ISQM conformant quality assurance program. The ISQM conformity program is patterned upon three (3) of five (5) Tiers of Approval described in Appendix 1-1-A4 of the *ABS Rules for Conditions of Classification (Part 1)* (Part 1 of the *ABS Rules for Building and Classing Steel Vessels (Steel Vessel Rules)*) and Appendix 1-1-A3 of the *ABS Rules for Conditions of Classification – Offshore Units and Structures (Part 1)* (Part 1 of the *ABS Rules for Building and Classing Mobile Offshore Drilling Units (MODU Rules)*). Although ABS does not offer type approval for software, Approval Tiers 1, 2 and 5 of the Steel Vessel Rules Type Approval are well suited for software quality management process certification, and are applied with certain alterations to the ABS ISQM Conformity Certification program. For comparison, Table 1 indicates the Tiers applicable to Steel Vessel Rules Approval and the Tiers applicable to the ISQM Conformity Certification.

TABLE 1
ISQM Conformity Program Based on Steel Vessel Rules Approval Tiers

Steel Vessel Rules Approval Tiers		ISQM Certification Tiers	
Tier 1	Manufacturer's Certification (MC)	Tier 1	<i>Manufacturer's Certification (MC)</i>
Tier 2	Product Design Assessment (PDA)	Tier 2	<i>Product Design Assessment (PDA)</i>
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	<i>Unit Certification via Survey During Final Test (UC)</i>

These Guidance Notes become effective on the first day of the month of publication.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of these Guidance Notes is the most current.

We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.

Terms of Use

The information presented herein is intended solely to assist the reader in the methodologies and/or techniques discussed. These Guidance Notes do not and cannot replace the analysis and/or advice of a qualified professional. It is the responsibility of the reader to perform their own assessment and obtain professional advice. Information contained herein is considered to be pertinent at the time of publication, but may be invalidated as a result of subsequent legislations, regulations, standards, methods, and/or more updated information and the reader assumes full responsibility for compliance. This publication may not be copied or redistributed in part or in whole without prior written consent from ABS.



GUIDANCE NOTES ON

SOFTWARE PROVIDER CONFORMITY PROGRAM

ABS CyberSafety™ VOLUME 5

CONTENTS

SECTION 1	Introduction	1
1	Software Quality.....	1
1.1	Introduction.....	1
3	Three Tiers of Software Quality Assessment and Certification	2
3.1	Overview.....	2
3.3	Conformance to Quality Standards.....	6
3.5	Software Quality Activities and Metrics.....	7
5	Software Development Life Cycle.....	8
7	Scope of the Guidance Notes	9
9	Definitions and Abbreviations	9
9.1	Definitions.....	9
9.3	Abbreviations.....	10
TABLE 1	Three Tiers of ISQM Conformity	2
TABLE 2	ISQM Manufacturer's Certification	3
TABLE 3	ISQM Product Design Assessment.....	3
TABLE 4	ISQM Unit Software Certification	4
FIGURE 1	ISQM Guidance Notes	1
FIGURE 2	ISQM Conformity Certification Process	6
FIGURE 3	Software Development Life Cycle.....	9
SECTION 2	ISQM Product Design Assessment – Part 1.....	11
1	Introduction	11
1.1	Requesting a PDA-Part 1 Evaluation.....	11
1.3	Completing a PDA-Part 1 Evaluation.....	12
3	Project Management	13
3.1	Initiating Activities	13
3.3	Planning Activities.....	14
3.5	Execution and Monitoring	15
3.7	Control Activities.....	15
3.9	Closing Activities.....	16

5	Software Development.....	17
5.1	Design Group	17
5.3	Construction Phase	21
5.5	Verification, Validation, and Transition (V V&T) Phase	22
5.7	Operation and Maintenance	24
TABLE 1	ISQM Product Design Assessment Certification	11
FIGURE 1	ISQM – Conformity Process: ISQM-PDA-Part 1.....	12
FIGURE 2	Integrated Best Practices Approach: Project Management....	13
FIGURE 3	Integrated Best Practices Approach: Software Development.....	17
FIGURE 4	Integrated Best Practices Approach: Software Design Group	17
FIGURE 5	Integrated Best Practices Approach: Software Concept Development.....	18
FIGURE 6	Integrated Best Practices Approach: Software Requirements and Design	19
FIGURE 7	Integrated Best Practices Approach: Software Construction.....	21
FIGURE 8	Integrated Best Practices Approach: Software V V&T.....	23
FIGURE 9	Integrated Best Practices Approach: Software Operation and Maintenance	24

SECTION 3 ISQM Product Design Assessment – Part 2..... 26

1	Introduction	26
1.1	Requesting a PDA-Part 2 Evaluation	27
1.3	Completion of the PDA-Part 2 Evaluation.....	29
3	Project Management.....	29
3.1	Initiating Activities.....	29
3.3	Planning Activities	30
3.5	Execution and Monitoring.....	31
3.7	Control.....	32
3.9	Closing	33
5	Software Development.....	33
5.1	Design Group	34
5.3	Construction	39
5.5	Verification, Validation, and Transition	44
5.7	Operation and Maintenance Phase	46
7	Product Design Assessment Renewal.....	47
7.1	Introduction.....	47

TABLE 1	ISQM Product Design Assessment Certification	26
---------	--	----

FIGURE 1	PDA-Part 2 Certification Process.....	27
----------	---------------------------------------	----

FIGURE 2	Integrated Best Practices Approach: Project Management....	29
----------	--	----

FIGURE 3	Integrated Best Practices Approach: Software Development	34
FIGURE 4	Integrated Best Practices Approach: Software Design Group	34
FIGURE 5	Integrated Best Practices Approach: Software Concept Development	34
FIGURE 6	Integrated Best Practices Approach: Software Requirements and Design	35
FIGURE 7	Integrated Best Practices Approach: Software Construction	39
FIGURE 8	Integrated Best Practices Approach: Software V V&T	44
FIGURE 9	Integrated Best Practices Approach: Software Operation and Maintenance	46
FIGURE 10	PDA Renewal Process	48
SECTION 4	Unit Software Certification (USC)	49
1	Introduction	49
3	Supplier Preparation for Unit Software Certification	49
3.1	Unit Software Certification	49
3.3	PDA Certification and USC	50
5	ABS Issuance of a USC Report or Letter to the Software Supplier	51
5.1	ABS Review of Final Test Procedure	51
5.3	ABS Witnessing of the Software System Final Test	51
5.5	System Provider Final Test Report	51
5.7	ABS-issued Unit Software Certification	51
TABLE 1	ISQM Unit Software Certification	49
FIGURE 1	ISQM Unit Software Certification	50
APPENDIX 1	Recommended References	52
APPENDIX 2	ISQM Software Quality Management – Certification Process	53
1	Tier 1 – Manufacturer’s Certification (MC)	53
1.1	ISQM PDA Certification Process Requires a Manufacturer's Certification (MC)	53
1.3	No ABS Certificate is issued	53
3	Tier 2 – ISQM PDA Certification Process	53
3.1	Supplier Initiates ISQM PDA-Part 1 Certification Process	53
3.3	ABS Performs Off-Site PDA-Part 1 Review of Supplier Software Quality Engineering Documentation	53
3.5	ABS Performs a PDA-Part 1 On-Site Assessment of Conformity to Supplier Software Quality Engineering Documentation.	54
3.7	ABS Issues a PDA Certificate	56
3.9	ABS Performs a PDA Certificate 2-Year Periodic Renewal Assessment	56
3.11	ABS Performs a Non-periodic PDA Certificate Assessment as Required to Verify Continued Conformity	57

5	Tier 5 – Unit Software Certification (USC) Assessment	57
5.1	Vessel Owner/Operator Initiates an ABS Unit Software Certification with ABS	57
5.3	ABS Witnesses the On-Site Test of the Named Product(s)	58
5.5	ABS Issues the USC Letter	58
APPENDIX 3 Sample ISQM-PDA-Part 1 Letter of Completion		59
APPENDIX 4 Sample PDA Certificate		61
APPENDIX 5 Sample Unit Software Certification		63
APPENDIX 6 ISQM Conformity Certification Process		66

This Page Intentionally Left Blank

.....



SECTION 1 Introduction

1 Software Quality

1.1 Introduction

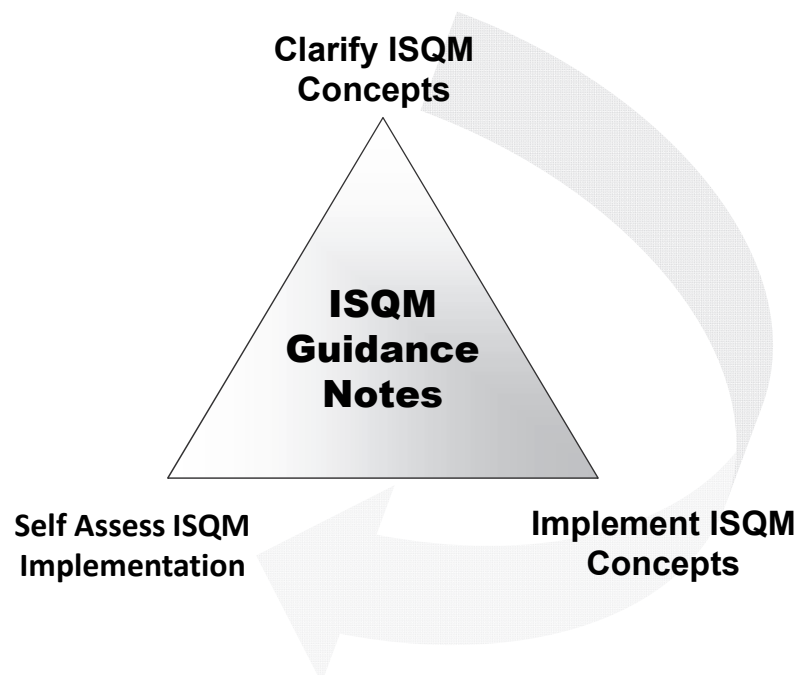
The intended outcome of applying the American Bureau of Shipping (ABS) ISQM program to software development include improving the quality of software in the marine and offshore industries; expedited reviews and approvals; and providing a level of confidence that products available from the System Providers (SP) are developed so as to meet the minimum quality requirements set forth in the *ABS Guide for Integrated Software Quality Management (ISQM) (ISQM Guide)*.

ISQM practices and processes are provided to help the SP establish a program that reinforces quality in the configuration and development of control system software. In addition to direct and specific application of ISQM to improve the quality of software, the SP may also find it useful to map internally developed quality assurance practices to those described in the *ISQM Guide*. By doing so, the SP can internally evaluate and measure its conformity to ISQM.

ABS has developed these Guidance Notes for managers, quality management personnel, and software developers engaged in software development or software quality assurance within SP organizations. These Guidance Notes are provided to:

- i) Clarify the evaluation processes required for ABS conformity recognition
- ii) Offer additional information to help the SP implement the ISQM principles
- iii) Assist the SP in evaluating its conformity to the *ISQM Guide*

FIGURE 1
ISQM Guidance Notes



3 Three Tiers of Software Quality Assessment and Certification

3.1 Overview

The ISQM conformity program is patterned upon three (3) of five (5) Tiers of Approval described in Appendix 1-1-A4 of the *ABS Rules for Conditions of Classification (Part 1)* (Part 1 of the *ABS Rules for Building and Classing Steel Vessels (Steel Vessel Rules)*) and Appendix 1-1-A3 of the *ABS Rules for Conditions of Classification – Offshore Units and Structures (Part 1)* (Part 1 of the *ABS Rules for Building and Classing Mobile Offshore Drilling Units (MODU Rules)*). Although ABS does not offer type approval for software, Approval Tiers 1, 2 and 5 of the *Steel Vessel Rules* are well suited for software quality management process certification, and are applied with certain alterations to the ABS ISQM Conformity Certification program (Section 1, Table 1). For comparison, Section 1, Table 1 indicates the certification Tiers applicable to Steel Vessel Rules Type Approval (Section 4-9-3¹), MODU Rules Type Approval (Section 4-3-4/5², Section 6-1-5³) and ISQM Conformity Certification.

TABLE 1
Three Tiers of ISQM Conformity

Steel Vessel Rules Approval Tiers		ISQM Certification Tiers	
Tier 1	Manufacturer's Certification (MC)	Tier 1	<i>Manufacturer's Certification (MC)</i>
Tier 2	Product Design Assessment (PDA)	Tier 2	<i>Product Design Assessment (PDA)</i>
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	<i>Unit Certification via Survey During Final Test (USC)</i>

Demonstration of ISQM conformity by the supplier is recognized by ABS through the issuance of:

- i) A *Manufacturer's Certification Letter of Acknowledgement* – Tier 1 conformity approval patterned upon the *ABS Rules for Conditions of Classification (Part 1)*;
- ii) A Product Design Assessment (PDA) certificate – Tier 2 conformity approval patterned upon the *ABS Rules for Conditions of Classification (Part 1)*; and,
- iii) A Unit Software Certification (USC) report – Tier 5 conformity approval patterned upon the *ABS Rules for Conditions of Classification (Part 1)*.

ABS does not provide software approval for Tier 3 – Type Approval, or Tier 4 – Product Certification via Product Quality Assurance (PQA), as defined in the *ABS Rules for Conditions of Classification (Part 1)*. Type Approval of software products is not applicable because software is not “manufactured” in the conventional sense. Software is also subject to customization and frequent changes through field-installed updates and defect fixes, which makes Type Approval inappropriate for software. Additionally, Product Certification via PQA is conventionally applicable to Mass Produced Products, which is a process not commonly applied to software systems. Therefore, neither Tier 3 nor Tier 4 approval are applied to ISQM Conformity Certification.

3.1.1 Tier 1: Manufacturer's Certification (MC)

The System Provider (SP) initiates Tier 1 approval by notifying ABS of its desire to be assessed for conformity to ISQM USC or the ISQM PDA. At the same time, the SP provides a letter to ABS asserting or certifying that it implements an ISO 9001 quality management program or a recognized equivalent. ABS acknowledges receipt of the SP-provided Manufacturer's Certification, and collaborates with the SP to initiate the ABS USC or the ISQM PDA conformity certification assessment. No ABS certificate is issued, and ABS does not perform a quality management documentation review or on-site assessment in connection with the MC. The SP's documentary

¹ ABS *Steel Vessel Rules*, 2012; 4-9-3/1: “Computer based systems where used for control, monitoring and safety systems are to comply with the provisions of Section 4-9-3, and are subject to the classification requirements regardless of **ACC** or **ACCU** notation, see 4-9-3/Table 1 for examples. See 4-9-1/7.3.9 for plans and data to be submitted for review.”

² ABS *MODU Rules*, 2016; 4-3-4/5: “Computer-based systems are to meet the requirements of 4-9-3/3 of the *Steel Vessel Rules*, even when the drilling unit will not be assigned with **ACC** or **ACCU** notations.”

³ ABS *MODU Rules*, 2016; Section 6-1-5: Survey and Certification

evidence that supports quality management certification is “M” classification documentation, and is to be kept by the SP and made available for review as requested by ABS. For additional information on documentation management refer to Section 4-9-3 of the *Steel Vessel Rules*, “M = Evidence kept by manufacturer and upon request checked by ABS.”

TABLE 2
ISQM Manufacturer’s Certification

Steel Vessel Rules Approval Tiers		ISQM Certification Tiers	
Tier 1	Manufacturer’s Certification (MC)	Tier 1	Manufacturer’s Certification (MC)
Tier 2	Product Design Assessment (PDA)	Tier 2	Product Design Assessment (PDA)
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	Unit Certification via Survey During Final Test (USC)

3.1.2 Tier 2: ISQM Product Design Assessment

The ABS PDA for software is organized as two parts. Both parts are to be completed by the SP before an ABS ISQM PDA is issued. Part 1 is an offsite review of software quality engineering process documentation. Part 2 is an onsite assessment of the SP’s implementation of its software quality process, and includes interviews with project management, quality and software development teams.

TABLE 3
ISQM Product Design Assessment

Steel Vessel Rules Approval Tiers		ISQM Certification Tiers	
Tier 1	Manufacturer’s Certification (MC)	Tier 1	Manufacturer’s Certification (MC)
Tier 2	Product Design Assessment (PDA)	Tier 2	Product Design Assessment (PDA)
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	Unit Certification via Survey During Final Test (USC)

3.1.3 Tier 2: Product Design Assessment – Part 1

The ISQM PDA-Part 1 assessment is a review of software quality management documentation pertinent to the software products to be named in the PDA or the USC. The ISQM-PDA-Part 1 assessment is an ABS review for indications that the SP possesses knowledge of the ISQM Guide, has implemented software quality management practices that conform to the ISQM Guide and recognized best practices, and has mapped its software quality processes to those described in these Guidance Notes in order to facilitate the assessment. The SP’s software quality engineering documentation is “S” classification documentation, and is checked by ABS. For additional information on documentation management refer to Section 4-9-3 of the *Steel Vessel Rules*, S-category of documentation: “S = Evidence to be checked by ABS.”

SP provided documentation is also reviewed for indications that formally documented software development life cycle development procedures, risk assessment and management procedures (i.e., safety reviews, FMEA or FMECA, revision control, etc.), and rigorous testing procedures (i.e., verification and validation) are in place.

The ISQM-PDA-Part 1 assessment is concluded after the ABS documentation review is complete, findings are reported to the SP. And the Findings are remedied by the SP. ABS’ findings are communicated to the SP in a findings review meeting. To proceed to ISQM PDA-Part 2, the SP corrects any findings (shortfalls in process, procedure, or documentation) communicated by ABS.

The SP is allowed six (6) months from the date of ABS' findings communication meeting to respond to ABS with its remedies to findings. If ABS approves the remedies provided in the SP's response, the SP is issued an ISQM-PDA-Part 1 completion letter. From this point in the PDA assessment, the supplier may proceed with the PDA-Part 2 assessment in pursuit of an ISQM Product Design Assessment (PDA) Certification.

In the event the SP does not provide documentation to ABS that demonstrates remediation of ABS findings within the six-month period following the ISQM-PDA-Part 1 findings communication, the SP may not initiate a PDA-Part 2 assessment.

3.1.4 Tier 2: Product Design Assessment – Part 2

In continuation of the ISQM PDA assessment process, ABS provides the Product Design Assessment – Part 2 to document that ABS has reviewed the application-in-practice of the SP's quality processes, procedures, and tools in conformity to the *ISQM Guide* and these Guidance Notes. The PDA-Part 2 pertains only to the specific site, development team, and software products reviewed during the assessment.

ABS' PDA certification process includes an on-site assessment for conformance of the SP's implementation of quality processes in practice to the *ISQM Guide* and in these Guidance Notes. With special considerations by ABS, the assessment may also include an evaluation of the documents describing a previously completed project to which ISQM-mapped quality processes were applied. In this assessment, ABS witnesses a final integration/acceptance test and reviews a final report addressing any exceptions noted in the test. In the event that the Owner requests the SP to assign a unit/vessel number to the product as tested and witnessed, ABS may also provide a Unit Software Certification (USC) documenting that ABS witnessed the test of a specific product for a specific customer and application (typically a vessel or unit) as assigned.

Based on successful completion of the PDA-Part 2 assessment, the SP is issued an ISQM-PDA certificate that is published on the ABS website. This ISQM-PDA certification may be renewed every two years based on an ABS on-site assessment of the SP's software quality practices, with special considerations by ABS. Failure to complete a timely renewal of the PDA will result in expiration of the PDA and removal of the certificate from ABS' website.

3.1.5 Tier 5: Unit Software Certification (USC)

ABS issues the USC to an Owner and/or Operator of a vessel on which a specified software product is to be installed or deployed. The USC is provided after ABS receives an SP-provided MC letter, reviews pertinent software quality engineering documentation and witnesses a successful onsite final product test. The SP's software quality engineering USC documentation is "S" classification documentation, "S = Evidence to be checked by ABS." The final product test is witnessed by ABS, and is a "W" classification system test, "W = To be witnessed" by the ABS assessor. For additional information on documentation management refer to Section 4-9-3 of the *Steel Vessel Rules*.

TABLE 4
ISQM Unit Software Certification

Steel Vessel Rules Approval Tiers		ISQM Certification Tiers	
Tier 1	Manufacturer's Certification (MC)	Tier 1	Manufacturer's Certification (MC)
Tier 2	Product Design Assessment (PDA)	Tier 2	Product Design Assessment (PDA)
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	Unit Certification via Survey During Final Test (USC)

To initiate the USC, the Owner/Operator instructs the SP to notify ABS that the Owner/Operator is requesting a USC for a specified software product to be installed on a specified vessel. The SP provides an MC letter to ABS as well as pertinent product software quality engineering documents requested by ABS. The documents are reviewed offsite by ABS prior to the onsite witnessing of the final product test. The documents reviewed minimally include:

- The SP's software quality engineering policies and procedures
- Product's Functional Description Document (or ConOps, SRS and SDS) as described in the *ISQM Guide*
- Product safety review, FMEA and/or FMECA documentation
- Software management of change and configuration management policy and procedures
- Detailed test plan

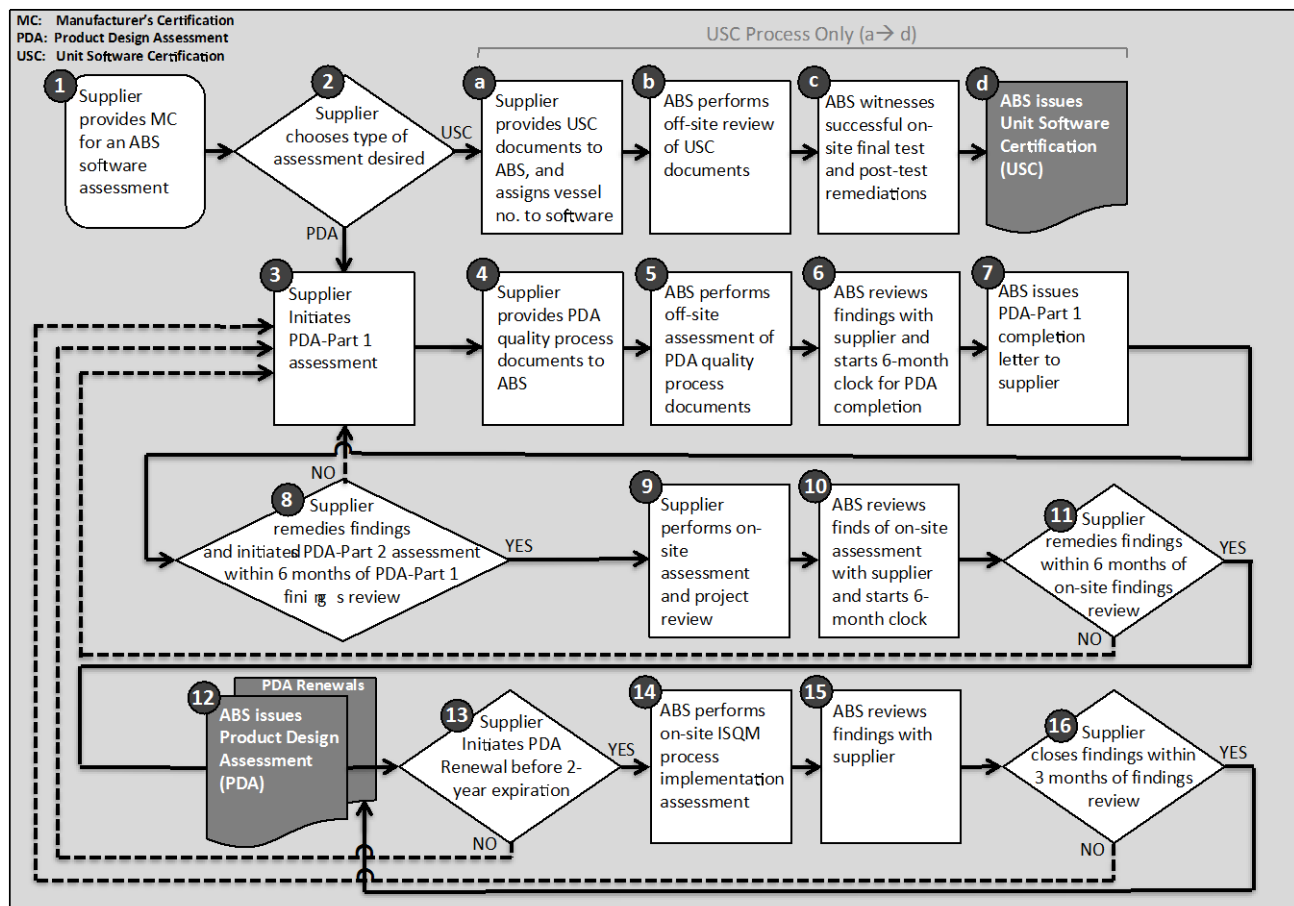
During the USC test activity, an ABS assessor witnesses the final product test (typically at the supplier site) of the software system being assessed for USC, witnesses meetings in which test issues are resolved with the Owner/Operator, witnesses any required retesting, reviews the SP's final test report, and responds to the SP and Owner/Operator with an ABS ISQM test report. If the software quality engineering documentation, test plan, test process, test outcomes, and final test report conform to ISQM practices, ABS provides a USC letter to the Owner/Operator that specifically names the equipment for which Owner requests certification.

The SP may elect to combine USC survey activities with PDA certification activities in order to efficiently and effectively demonstrate implementation of its software quality engineering processes

3.1.6 ISQM Conformity Certification Process Workflow

The ABS process for providing the three tiers of ISQM certification is provided in Section 1, Figure 2. In the conformity certification process graphic, the normal process flow is depicted as solid lines, and the remedial process flow is depicted as dashed lines.

FIGURE 2
ISQM Conformity Certification Process



3.3 Conformance to Quality Standards

Conformance to both explicit and implicit requirements as represented in specifications embodies the concept of quality for software. Explicit requirements as stated in specifications include the system's functional and performance criteria as guided by development (coding) standards – whether explicitly stated in the specification, or implicitly expected as inherent in quality software. Implicit requirements also include less quantifiable, but important operational and business software characteristics. Satisfaction of both explicit and implicit requirements, as verified in thorough system testing, combine to represent total software quality.

The three key points in this expression of software quality are:

- i) Delivered software complies with the stated requirements;
- ii) Delivered software is developed using appropriate development criteria (coding requirements) and specifications (user requirements); and,
- iii) Delivered software meets implicit requirements.
 - Implicit or extra-functional requirements are expected by the user to be satisfied in delivered software; however, those requirements may not be included in the coding specification. Examples of implicit (extra-functional) requirements include but are not limited to security, stability, usability, reliability, maintainability, testability, evolvability, etc.⁴
- iv) If software conforms to its explicit requirements but fails to meet implicit requirements, software quality may be perceived as lacking.

⁴ In software discussions, implicit requirements are sometimes referred to as the "...ilities" of requirements.

The IEEE Standard for Software Quality Assurance Plans, 730-2002 provides guidance and details on Software Quality Assurance (SQA) organizations, activities, documents, reviews, etc.

- i) Quality is defined as the sum total of characteristics and performance of a product or service that satisfies the stated or implied needs of customers. Viewpoints and relative importance concerning quality vary with respect to the different factors considered.
 - The Owner's viewpoint may consider global quality, wherein the highest quality possible is provided within the selected equipment.
 - The developer's viewpoint may consider adherence to and satisfaction of specifications throughout the software development life cycle, which in turn yields a high quality final product.
 - The Operator's viewpoint may consider operational quality as characterized by consistent, predictable, safe performance of work by the integrated system throughout its specified operating life.
- ii) Software quality is also characterized by how the software:
 - Is designed (quality of design);
 - Accurately resolves the design as software code (i.e., accuracy of coding execution); and
 - Operates in the environment for which it is intended by faithfully fulfilling user needs and/or requirements.

3.5 Software Quality Activities and Metrics

3.5.1 Management

The most basic quality management requirements are to:

- Plan the project quality processes,
- Execute to the project according to the quality processes as planned, and
- Evaluate both the outcomes of the project and the execution of the project plan.

3.5.2 Planning

The IEEE Standard for Software Quality Assurance Plans, 730-2002 provides a table suggesting artifacts that are applicable in each of the SDLC phases. These include:

- Plans
- Specifications
- Descriptions
- Procedures
- Reports
- Records

3.5.3 Execution

Key to the execution of the plan is a well-developed functional test strategy. Referencing the IEEE 730 standard can guide a development organization and testers through a series of procedures and tests that are applicable to the system under development.

Peer reviews are effective for evaluating the software modules of individual development activities. These reviews are performed by development peers who check for compliance with a quality plan and development standards, for adherence to specification, and for comprehension of requirements. Also commonly referred to as "code walkthroughs", peer reviews as provided for in the IEEE Standard for Software Reviews 1028-1997, are defined as a process "...in which a designer or programmer leads members of the development team and other interested parties through a software product, and the participants ask questions and make comments about possible errors, violation of development standards, and other problems".

Project control review processes as suggested by the Project Management Institute's (PMI) Project Management Book of Knowledge (PMBOK®) are also useful for control of a software project. Reviews such as Preliminary Design Reviews and Critical Design Reviews are techniques used to evaluate both the cost and progress toward the schedule of a project. These reviews also provide opportunities to evaluate the execution of the quality plan.

3.5.4 Evaluation

Software quality evaluation includes techniques and operational activities that are used to control the accurate fulfillment of quality requirements. It involves an assessment of product quality relative to the initial quality requirements, and as-required adjustments to the product design and the project execution process. Variances from quality requirements discovered early in the development process have a smaller impact upon the project than variances discovered late in the project, and they typically have a much smaller impact than variances discovered after the product is placed in the field.

Product quality evaluation is performed through verification and validation activities, which are done in consideration of the various expectations and viewpoints of the owner, system developer, and operator. The differing viewpoints (owner, developer and operator) provide the aggregate basis for quality evaluation.

Verification is typically done by testing system components, by testing the integration of system components, by reviewing the veracity of potential test models, and by testing the performance of the final product. The system delivery group performs testing in conjunction with system verification and is responsible for the delivery of a software system that meets quality requirements.

Validation is typically done using prototyping and product review techniques and again during installation and integration at the vessel or unit. Documented requirements traceable to specifications and the specific tests performed commonly provide essential information when validating comprehensive satisfaction of user requirements in the delivered product.

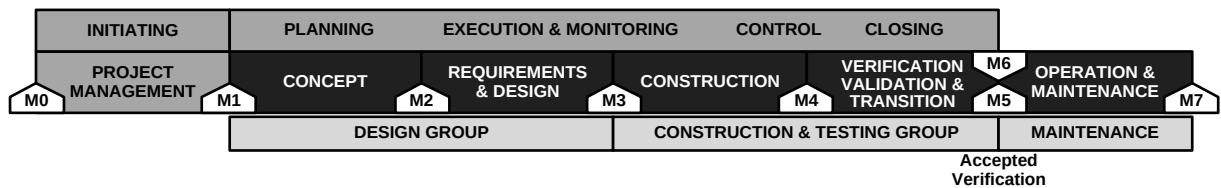
3.5.5 Measurement

Quantitative measurement is central to achieving and improving software quality. Software quality is commonly attributed to software that achieves measurable attributes, such as Mean-Time-To-Failure (MTTF) and Fielded Errors. A failure is construed as an event in which the control system's programming causes the Equipment Under Control (EUC) to perform an action that is unpredicted, undesired, unsafe, etc. A fielded error is commonly construed as a software defect discovered after the software has been delivered to the customer. The SP typically collects and analyzes data to assist in evaluating software quality and reserves those metrics for proprietary quality analytics. While ABS encourages the use of quantitative software quality measurement techniques, the methods and results of quality measurement are left to the SP and are considered proprietary.

5 Software Development Life Cycle

The Software Development Life Cycle (SDLC) as shown in Section 1, Figure 7 is the seminal representation of ABS' ISQM process as presented in the *ISQM Guide*. It is the map of ABS' ISQM program, and provides the basic structure for guiding the discussion of software quality in this document. Each phase of project management and software development processes are addressed by this graphic. It establishes the logical framework by which the critical elements of the SP's quality practices and policies are implemented and assessed. This software life cycle process has been refined and successfully used for years in many industries to develop well-engineered software products. For the convenience of the reader, this graphic is presented repeatedly to illuminate the discussion in each section of these Guidance Notes.

FIGURE 3
Software Development Life Cycle



7 Scope of the Guidance Notes

These Guidance Notes describe a number of recommended best practices for software quality management, as well as software quality management concepts based on research and industry convention. This convention indicates that rigorous project management and disciplined software engineering practices have a positive impact on the quality of software. The SP is encouraged to reference the *ISQM Guide*, the practices offered in this document, and the references cited in both documents when pursuing ABS ISQM certifications.

These Guidance Notes are organized in four major sections so as to be usable whether read “straight through” or referred to in sections.

- Section 1 provides a summary overview of the three tiers of ABS assessment and associated certifications for software: Manufacturer’s Certification, PDA-Parts 1 and 2, and Unit Software Certification.
- Section 2 provides guidance to the SP for demonstrating conformity to the *ISQM Guide* in its Software Quality Assurance (SQA) process documentation during the PDA-Part 1 assessment, which in turn enables the SP to proceed to the PDA-Part 2 assessment.
- Section 3 provides guidance to the SP for demonstrating sufficient conformity to the *ISQM Guide* in its Software Quality Assurance practices during the PDA-Part 2 assessment, which results in issuance of ABS’ Product Design Assessment (PDA) certification for the software explicitly named by product, the assessed software development team, and the assessed production location. Section 3 also provides information about PDA renewal.
- Section 4 provides guidance to the SP for obtaining ABS’ Unit Software Certification for specific software systems that are to be installed on a specific unit or vessel.

Each Section of these Guidance Notes maps its content to Section 1, Figure 3, and presents useful examples and recommendations of both Project Management and Software Engineering practices and concepts in support of the *ISQM Guide* and ABS’ software certifications. The reader should note that the PDA certification process is cumulative.

9 Definitions and Abbreviations

9.1 Definitions

Artifacts: Objects, documents, and data produced by efforts of personnel assigned to software projects.

Malware, Malicious Code, and Malicious Software: A software program (e.g., viruses, worms, Trojan horses, backdoors, keystroke loggers, phishing, hoaxes, etc.) that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system.⁵

Software: Internally developed programming satisfying the required functionality that meets specifications requested by the shipyard, owner, or operator.

Supplier: The designation used in process graphics and certification letters to represent a System Provider (SP) and Connected Equipment providers.

⁵ NIST Special Publication 800-83r1, Guide to Malware Incident Prevention and Handling, 2013

9.3 Abbreviations

<i>ConOps:</i>	Concept of Operation Document
<i>CM:</i>	Software Configuration Management
<i>COTS</i>	Commercial-off-the-shelf equipment or solutions
<i>EUC:</i>	Equipment Under Control
<i>FDD</i>	Functional Description Document
<i>HMI</i>	Human Machine Interface
<i>IL:</i>	Integrity Level assigned by the owner (see <i>ISQM Guide</i> , Section 3)
<i>ISQM Guide:</i>	<i>ABS Guide for Integrated Software Quality Management (ISQM)</i>
<i>MC:</i>	Manufacturer's Certification
<i>PDA:</i>	ABS Product Design Assessment (Certificate). For this specific PDA is issued when upon completion of PDA-Part 1 and PDA-Part 2 assessments
<i>PDA-Part 1:</i>	ISQM Conformity Certification Process during which SQA process documentation is assessed for conformity to the <i>ISQM Guide</i> and these Guidance Notes
<i>PDA-Part 2:</i>	ISQM Conformity Certification Process during which SQA process implementation is assessed for conformity to the <i>ISQM Guide</i> and these Guidance Notes
<i>PM:</i>	Project Management
<i>PMBOK®:</i>	Project Management Body of Knowledge
<i>PQA:</i>	Product Quality Assurance
<i>Secondary Entity:</i>	A supplier providing product and/or services to a System Provider (SP), a sub-contractor
<i>SDLC:</i>	Software Development Life Cycle
<i>SDS:</i>	Software Design Specification
<i>SP:</i>	System Provider of control systems for major hardware, and the entity having legal or patent rights to produce a software product or system
<i>SQA:</i>	Software Quality Assurance
<i>SRS:</i>	Software Requirement Specification
<i>TEP:</i>	Test and Evaluation Plan
<i>USC:</i>	Unit Software Certification
<i>V&V Plan:</i>	Verification and Validation Plan to include any commissioning/integration-testing plan(s)
<i>WBS:</i>	Work Breakdown Structure
<i>W-3:</i>	"What-When-Who"; a project management expression of "What is done When, and by Whom".



SECTION 2 ISQM Product Design Assessment – Part 1

1 Introduction

The first step of the ABS PDA process for software is a review of ISQM software quality processes and procedures as documented for use by an SP's software development organization during the development and deployment of software products for a given application. The PDA-Part 1 process in Section 2, Table 1 is shown in detail in Section 2, Figure 1.

TABLE 1
ISQM Product Design Assessment Certification

Steel Vessel Rules Approval Tiers		ISQM Certification Tiers	
Tier 1	Manufacturer's Certification (MC)	Tier 1	<i>Manufacturer's Certification (MC)</i>
Tier 2	Product Design Assessment (PDA)	Tier 2	<i>Product Design Assessment (PDA)</i>
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	<i>Unit Certification via Survey During Final Test (USC)</i>

The PDA-Part 1 review concludes with documented findings concerning conformity of the SP's quality management processes to the information presented in the *ISQM Guide*. The findings contain ABS reviewer conclusions about the completeness and conformity of SP-documented software quality management processes, and procedures relative to the information presented in the *ISQM Guide*. The findings emphasize gaps or shortfalls found in SP's process documentation based on a comparison of that documentation to the processes or documentation included in the *ISQM Guide*.

1.1 Requesting a PDA-Part 1 Evaluation

1.1.1 Use of a Secondary Entity for Production of Software

A Product Design Assessment certification may only be issued to the original System Provider (SP). The SP is the entity possessing legal or patent rights to produce the software product or system.⁶ ABS considers the SP to be responsible for the continued conformity of named products listed in the PDA.

If the SP engages a secondary entity for production, maintenance, or support of products named for PDA, then that secondary entity is to be included in the PDA-Part 1 assessment. This secondary assessment is performed at an increased level of effort and cost to be defined as part of the assessment initiation contracting process between the SP and ABS.

- i) The SP is to provide written notification to ABS that a secondary SP entity (i.e., another internal group or third-party provider that is not collocated with the primary group being assessed) engages in the production or support of software products named for assessment and is participating in the PDA assessment. The notification is to include the name, address, and business relationship of the secondary entity.

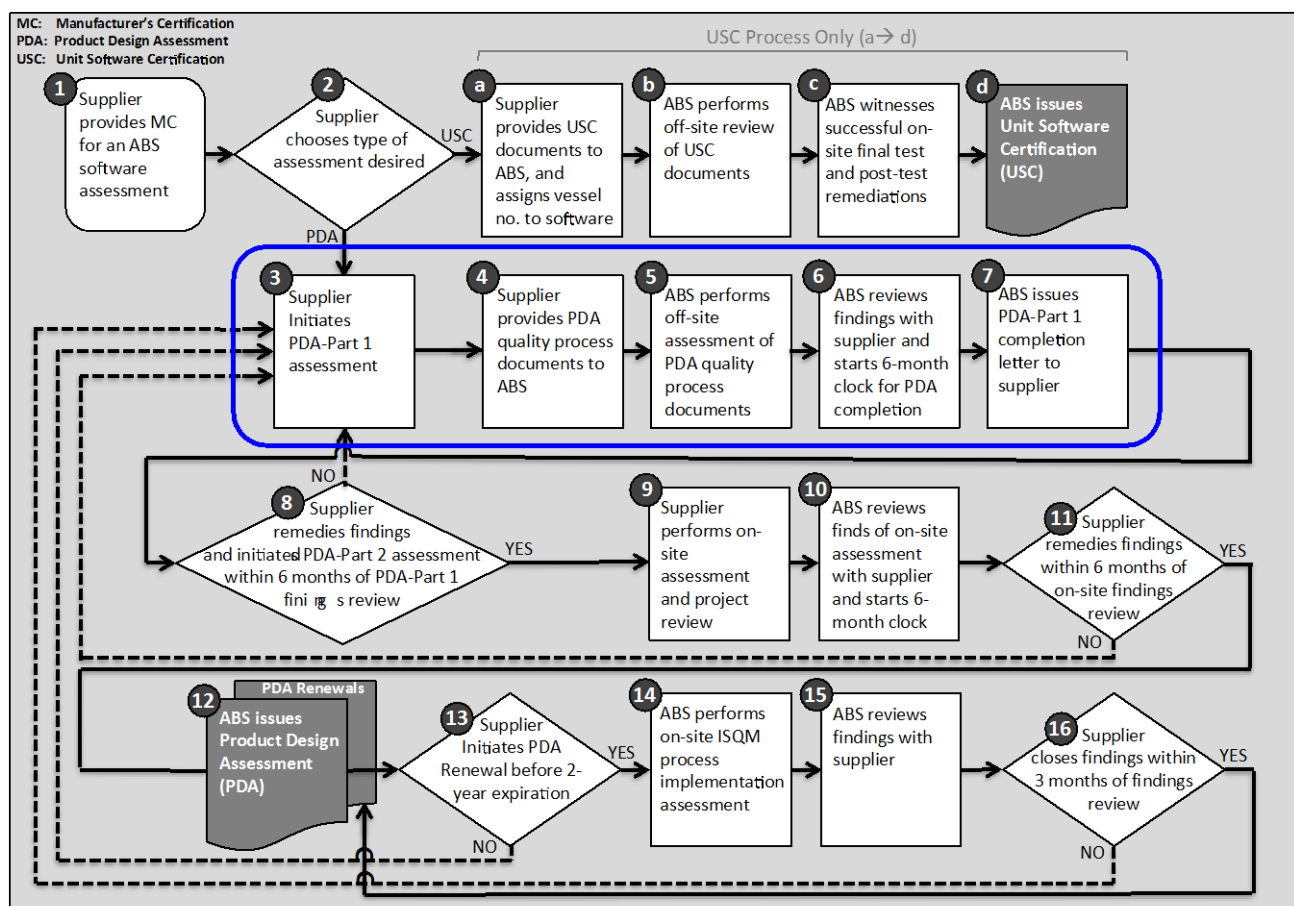
⁶ 1-1-A3/5.1.1 of the *ABS Rules for Conditions for Classification*: "A Product Design Assessment (PDA) may only be issued to the Designer or the Original Equipment Manufacturer (OEM). This is the entity that has legal or patent rights to produce the material, component, product or system. ABS will consider the Designer or the OEM to be responsible for the continued compliance of the PDA as assessed."

- ii) A secondary entity is to request an ABS conformity review, and provide documented SP approval of the secondary entity's participation in the review. The request is to also contain SP authorization for the secondary entity to provide SP documentation (hardcopy or electronic) that may be requested by ABS for PDA-Part 1 review.

1.3 Completing a PDA-Part 1 Evaluation

In order to successfully complete the PDA-Part 1 process, the SP is to remedy non-conforming documentation assessment findings communicated to the SP by ABS in a findings review meeting. The SP is provided six-months to remedy findings. The remediation period begins on the date of the ABS findings review meeting. During that time, the SP is to (a) remedy any process or documentation findings (gaps) discovered during the assessment, and (b) initiate the PDA-Part 2 assessment. Upon ABS' review and acceptance of the SP's remediation and closure of the findings, the successful completion of the PDA-Part 1 process is acknowledged by ABS in a letter from ABS to the SP. Upon receipt of the PDA-Part 1 successful completion letter, the SP may proceed with the PDA Part 2 assessment toward completion of the PDA assessment process. If the SP does not present documentation of findings remediation and closure to ABS and initiate the PDA-Part 2 assessment within six months of the PDA-Part 1 Findings Review, the SP is to reschedule a PDA-Part 1 assessment and repeat the PDA process in its entirety.

FIGURE 1
ISQM – Conformity Process: ISQM-PDA-Part 1

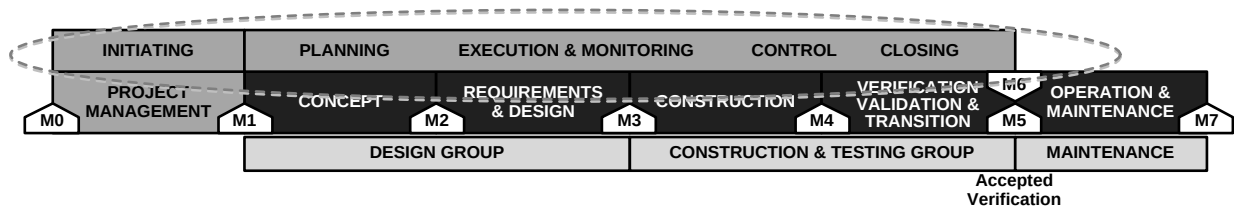


Section 3 of these Guidance Notes provides information that supports development of quality processes and procedure documentation in conformity with the *ISQM Guide* and issuance of the PDA-Part 1.

3 Project Management

This section provides guidance to the SP for reviewing critical Project Management (PM) processes for the ISQM-PDA-Part 1. Project management is considered important to the delivery of quality software and is highlighted in Section 2, Figure 2 as a set of processes that overarches the software development life cycle. The PDA-Part 1 review includes evaluation of process documentation that supports recognized project management practices that in turn support the development of quality software.

FIGURE 2
Integrated Best Practices Approach: Project Management



Project management practices as shown in Section 2, Figure 2 are executed concurrently with, and in support of the software development phases. Certain project management practices are positioned in close proximity to phases of the software development cycle in the above graphic. In practice however, the mapped phases of the PM cycle can also apply to each of the phases of the software development cycle. For example, each phase of the software development cycle has an initiation, planning, execution/monitoring, and closing (or handoff) phase – as does the entire software development cycle. Sound PM processes are useful in managing each phase of software development, and for the entire project, regardless of the development model used (e.g., waterfall, spiral, V-Model, etc.), and can clarify ISQM conformity when mapped to the software quality management processes presented in the *ISQM Guide*.

For each of the PM phases described below, these Guidance Notes provide quality practices that are reviewed as part of the PDA-Part 1 documentation evaluation.

3.1 Initiating Activities

In order for processes as presented by ABS' ISQM to be successfully implemented by the SP, the SP must first be aware of the contents of the *ISQM Guide*, and either develop a quality program based on the *ISQM Guide*, or map internally developed quality processes to ISQM processes. This level of awareness helps SP's management and individual contributors consider important quality questions and gain a deeper understanding of the processes that tend to characterize quality software development organizations. Process documentation described in the *ISQM Guide*, as well as processes described below, are considered during the PDA-Part 1 review of initiating documentation.

3.1.1 Quality Policy and Procedure Documentation

- i) The SP has mapped ABS' ISQM quality policies and procedures to internally developed software quality management processes, quality policies, and procedures.
- ii) Indication of conformity includes a detailed description of SP-developed software quality management processes, including a one-to-one mapping of internal processes and procedures to those in the *ISQM Guide*.

3.1.2 Awareness of Quality Policies Requirement

- i) The software development organization, including the project management and development teams, are aware of the company's policies and procedures.
- ii) Indications of conformity to the ISQM processes include a quality processes training program and a roster of project staff (by position and/or name) trained in quality practices and processes.

3.3 Planning Activities

The Planning Phase of a project demands that project activities are defined, that those activities are scoped and scaled so as to achieve project schedule objectives; that activity dependencies are sufficiently understood so as to give the schedule credibility; and, that each activity is the responsibility of a named person. In project management terminology, the assignment of “Activity” (What is done), “Responsibility” (Who does it), and “Delivery Date” (When it is done) is often referred to as “W-3’s”. Even basic project plans contain W-3’s in support of project clarity. The planning phase of a project also comprehends the risks to the success of the project product, project cost, and project schedule. Process documentation described in the *ISQM Guide*, as well as processes described below, are considered during the PDA-Part 1 review of planning documentation.

3.3.1 Project Roles

- i) Project roles, responsibilities, and authority are designated.
- ii) Indication of conformity includes designation of responsibility with process documentation assigning and explaining roles, responsibilities, and reporting structures.

3.3.2 Project Activities

- i) Project activities are identified and a project plan or Work Breakdown Structure (WBS) containing activity durations and dependencies is created and managed by means of a manual process or a computerized project management tool.
- ii) Indication of conformity includes a project work activity plan documented in a manual or computer-aided project planning system containing project activities, activity durations, activity dependencies, and completion milestones.

3.3.3 Risk Management

- i) A risk identification and management plan is in place for identifying and managing risks to both the specified software product performance and the required project execution performance.
- ii) Indication of conformity includes a document that describes:
 - Risks to meeting product specifications;
 - Risks to meeting project performance goals, such as delivery;
 - The probability that each risk will impact the project; and,
 - The risk management (mitigation or work-around) plan that is in place in the event the risk identified actually occurs.

3.3.4 Requirements Development

- i) Requirements acquisition, assessment, and documentation activities are scheduled in the system design phase of the software development cycle.
- ii) Indication of conformity includes a project schedule containing a requirements development activity; system design activity that supports the completion of the Design Group; a requirements traceability matrix showing how system requirements are tested for quality verification; and, related documentation outlined in the *ISQM Guide*. Collaboration meetings are scheduled for requirements acquisition with customers. Meeting minutes are captured, updated, and reviewed until action items are closed. [Best practice: The duration of the R&D Phase can be the longest software development life cycle phase in high performing organizations.⁷]

⁷ A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, 2012

3.5 Execution and Monitoring

Project execution and monitoring are dependent on the establishment and successful implementation of project initiation activities. Those processes and artifacts described in the preceding sections enable the SP to understand the requirements, define and plan project scope and schedules, assign tasks, evaluate progress, and take action to correct activities that do not follow the plan. Further, successful execution is often defined by a commitment to carefully monitor the “W-3’s” described above. Monitoring also maintains the integrity of the project planning process throughout the project life cycle. Process documentation described in the *ISQM Guide*, as well as processes described below, are considered during the PDA-Part 1 review of execution and monitoring documentation.

3.5.1 Schedule

- i) Project progress review meetings involving project stakeholders are routinely held by the SP.
- ii) Indications of conformity include ISQM collaboration activities in the project plan, frequent progress review meetings, and meeting minutes that document stakeholder participation, contributions of project collaborators, as well as action item lists that are maintained, updated, and archived.

3.5.2 Metrics

- i) Metrics and reports as prescribed in the *ISQM Guide* (see *ISQM Guide*, Appendix 8) are collected, maintained, and shared with appropriate members of the project team.
- ii) Indications of conformity include metrics templates, metrics monitoring reports, and presentations (e.g., quad-charts, stoplight charts, trend analyses, etc., containing ISQM reference metrics), as well as meeting minutes in which performance shortfalls are managed through corrective action reports, assignment of responsibilities, and due dates.
- iii) ABS does not review metrics data, but reviews documents for indications that metrics are being collected and analyzed.

3.7 Control Activities

Project control is differentiated from execution and monitoring. Execution and monitoring is the process by which information is gathered and organized so that project control (schedule and document management) is possible. In software projects, the term “control” commonly refers to the careful creation and archiving of software development artifacts (requirements, designs, and code) that describe the physical output resulting from the construction of software. Software project control is performed not only by control of the project management elements (W-3’s), but also through the implementation of formal documentation procedures, configuration management procedures, version control procedures, and processes or systems that manage the software as a physical product. Process documentation described in the *ISQM Guide*, as well as processes described below are considered during the PDA-Part 1 review of control activities documentation.

3.7.1 Revision Control

- i) A formal revision management procedure or system is used for requirements documentation management and design documentation management.
- ii) Indications of conformity include the documentation of a requirements and design version/revision control system and/or reports from that system, including traceability of requirements changes to design evolution.

3.7.2 Version Control

- i) A formal software version management procedure or system is used for managing revisions of code components and versions of the major software component (system), provides system evolution clarity and traceability, and includes version description documentation that accompanies each software release.
- ii) Indications of conformity include the documentation of the software development version and revision control system and/or documented reports from the system, including descriptions of version releases.