

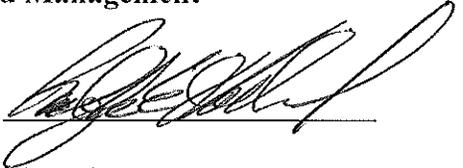
Date 8/5/2015



Environmental Management Consolidated Business Center (EMCBC)

Subject: Software Application Development and Management

Information Management Procedure

APPROVED: 

ISSUED BY: OFFICE OF INFORMATION RESOURCES MANAGEMENT

## 1.0 PURPOSE

The purpose of this procedure is to define the process for Non-Safety Software Application Development and Management, which includes integrating security functionality and assurance using system development life cycle (SDLC) management.

## 2.0 SCOPE

This procedure is for all applications developed by the Office of Information Resource Management (IRM) that utilize data management software such as MYSQL, ORACLE, SQL Server, etc.

## 3.0 APPLICABILITY

This procedure is applicable to all general application development activities. It is not applicable for applications requiring the development of a Major IT Business Case, formerly known as an Exhibit 300, (financial applications over \$5 million per year, other applications costing over \$5 million over three years, or designated "Critical Systems") or to Nuclear Safety or Safety Related Software. This procedure may be utilized for the development of systems that are designated as Software Quality Assurance Levels 3 and 4.

## 4.0 REQUIREMENTS and REFERENCES

### 4.1 Requirements:

- 4.1.1 Department of Energy, Environmental Management Risk Management Approach Implementation Plan (RMAIP) (<https://www.emcbc.doe.gov/msd/msd.php>)
- 4.1.2 PP-IRM-240-08, Cyber-Security-System Security Plan for General Support (<https://www.emcbc.doe.gov/msd/msd.php>)
  - 4.1.2.1 IA-6, Authenticator Feedback
  - 4.1.2.2 SA-4, Acquisition Process
  - 4.1.2.3 SA-11, Developer Security Testing
  - 4.1.2.4 SI-2, Flaw Remediation
  - 4.1.2.5 SI-3, Malicious Code Protection

4.1.2.6 SI-9, Information Input Restrictions

4.1.2.7 SI-10, Information Input Validation

4.1.2.8 SI-11, Error Handling

4.1.3 PO-IRM-240-06, Policy on the Control of Unclassified Electronic Information (<https://www.emcbc.doe.gov/msd/msd.php>)

## 4.2 References:

- 4.2.1 Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) -Application Security Checklist  
[http://iase.disa.mil/stigs/app\\_security/app\\_services/app\\_serv.html](http://iase.disa.mil/stigs/app_security/app_services/app_serv.html)
- 4.2.2 DOE O 414.1D, Quality Assurance  
(<https://www.directives.doe.gov/directives-documents/400-series/0414.1-BOrder-d-admchg1>)
- 4.2.3 DoD 5015.2-STD Electronic Records Management Software Application Design Criteria standard, 2007  
(<http://jite.fhu.disa.mil/projects/rma/standards.aspx>)
- 4.2.4 NQA-1 2004 Part II, SubPart 2.7  
(<http://energy.gov/management/downloads/nqa-1.pdf>)
- 4.2.5 NIST SP 800-64, Security Considerations in the System Development Life Cycle, October 2008 (<http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>)
- 4.2.6 Guide to IT Capital Planning and Investment Control (CPIC), September 2010 ([http://energy.gov/sites/prod/files/cioprod/documents/IM-20CPICBY2012\\_2\\_BUDGET.pdf](http://energy.gov/sites/prod/files/cioprod/documents/IM-20CPICBY2012_2_BUDGET.pdf))
- 4.2.7 IMP-IRM-8308-02, Configuration Management of Computer Systems and Networks (<https://www.emcbc.doe.gov/msd/msd.php>)
- 4.2.8 IMP-IRM-8308-05, Software Quality Assurance  
(<https://www.emcbc.doe.gov/msd/msd.php>)
- 4.2.9 Management System Description – SAP-OD-410B-07-Document Control Management, Procedure 7, Control of Technical Instruction Documents  
(<https://www.emcbc.doe.gov/msd/msd.php>)
- 4.2.10 PP-OTSAM-414-01, Quality Assurance Implementation Plan  
(<https://www.emcbc.doe.gov/msd/msd.php>)
- 4.2.11 Management System Description – Records Management  
(<https://www.emcbc.doe.gov/msd/msd.php>)
- 4.2.12 Management System Description – SAD-IRM-415, Applications and Software Development (<https://www.emcbc.doe.gov/msd/msd.php>)
- 4.2.13 36 CFR Part 1194 – Electronic and Information Technology Accessibility Standards (<http://www.gpo.gov/fdsys/granule/CFR-2011-title36-vol3/CFR-2011-title36-vol3-part1194/content-detail.html>)

## 5.0 DEFINITIONS

- 5.1 Alpha Testing: Testing of applications with inert data (made up data).
- 5.2 Beta Testing: Testing of applications with “real” data.
- 5.3 Content Manager: Individual assigned by the Content Owner to manage the development of the application and to ensure the integrity of the data.
- 5.4 Content Owner: The Assistant Director responsible for the content within the given application or system.
- 5.5 Data Sensitivity: Sensitivity of the data in accordance with the EMCBC Policy on the Control of Unclassified Electronic Information, PO-IRM-240-06. See Attachment A.
- 5.6 Data Set: The entirety of the type of data that the application will be manipulating including data type and sensitivity.
- 5.7 Data Type: Data within the EMCBC is classified by type according to the sensitivity of the data. Where data types are mixed, the most stringent control shall apply. See Attachment A.
- 5.8 Developer(s): IRM staff responsible for coding, testing, placing the application into production, and maintaining the application.
- 5.9 Independent Reviewer: Individual responsible for conducting the Software Quality Assurance Review when required. This individual shall not also act in any of the following roles: System Owner, Content Owner, Content Manager, or Developer for the application in question.
- 5.10 IRM Support Staff: IRM staff responsible for assisting in the completion of all required documentation related to the development and maintenance of an application.
- 5.11 Section 508 Compliance: Requires any application developed by the EMCBC to comply with requirements set forth in 36 CFR Part 1194 – Electronic and Information Technology Accessibility Standards unless compliance would cause an undue burden on the Agency.
- 5.12 Statement of Need: Defines what need is being fulfilled by the application. Address the functionality of the system, who needs to access the system, how often, and where they are located.
- 5.13 System Owner: The lead IRM individual that has overall implementation responsibility for any given application. Usually the Assistant Director for the Office of Information Resource Management (ADIRM).

## 6.0 RESPONSIBILITIES

- 6.1 System Owner shall:
  - 6.1.1 Approve the completed Application Project Plan (APP).

- 6.1.2 Establish the Data Base Management System and applicable user interface.
- 6.1.3 Provide the test and baseline actions required to certify or recertify the application for production.
- 6.1.4 Conduct a Make or Buy Analysis and, if applicable, oversee the procurement.
- 6.1.5 Include elements of Software Quality Assurance (SQA) applicable to specific projects as per IMP-IRM-8308-05, Software Quality Assurance.
- 6.1.6 Conduct annual application review.
- 6.1.7 Approve requests for software changes.
- 6.1.8 Conduct quarterly Application Project Plan (APP) Log reviews.
- 6.2 Content Owner or Manager (when assigned) shall:
  - 6.2.1 Submit a written request, hard copy or electronic, of the perceived need for a new application, which includes a Statement of Need, Data Type, and Data Sensitivity, to the ADIRM for determination of viability.
  - 6.2.2 Complete Checklists for Software Classification Determination, IMP-IRM-8308-03-F1, and Software Evaluation, IMP-IRM-8308-03-F2.
  - 6.2.3 Develop a flow chart of the business system that is being automated.
  - 6.2.4 Develop an analysis of the life cycle requirement for the application.
  - 6.2.5 Approve the proposed schedule for completion.
  - 6.2.6 Submit written requests, hard copy or electronic, for software changes to the Application Configuration Control Point Manager (CCPM) for processing and approval as per the Configuration Management of Computer Systems and Networks, IMP-IRM-8308-02.
- 6.3 Developer shall:
  - 6.3.1 Assist in the development of the APP.
  - 6.3.2 Develop a schedule for completion of the application.
  - 6.3.3 Develop the code for the application.
  - 6.3.4 Ensure that the application is brought into Configuration Management.
  - 6.3.5 Conduct testing and develop Baseline Change(s) as necessary. Testing will include compliance with Section 508 of the Rehabilitation Act of 1973.
  - 6.3.6 Resolve issues identified during Alpha and Beta testing.
  - 6.3.7 Complete testing documentation as required.
  - 6.3.8 Complete the baseline security for web applications as required.

- 6.3.9 Document all maintenance activities in the IRM Project Management System and/or Information Management (IM) Maintenance/Risk Log as required.
- 6.3.10 Complete required fields (e.g., code location, database, etc.) in APP Log.
- 6.3.11 Ensure APP Log is updated as necessary.
- 6.4 IRM Support Staff shall:
  - 6.4.1 Develop and complete the APP for approval.
  - 6.4.2 Maintain APPs and testing documentation for IRM.
  - 6.4.3 Develop changes and revisions to APP during the life cycle.
  - 6.4.4 Maintain APP Log. A hard-copy is available in the APP binder at the Data Center and an electronic copy is available in SharePoint.
- 6.5 Independent Reviewer shall:
  - 6.5.1 Approve the completed APP.
  - 6.5.2 Conduct Software Quality Assurance review when such a review is required.

**NOTE:** The individual assigned as the Independent Reviewer shall not also act in any of the following roles: System Owner, Content Owner, Content Manager, or Developer for the application in question.

## 7.0 GENERAL INFORMATION

This procedure provides for a structured process for the inception, design, development, and testing of applications developed by the EMCBC. The intent of this procedure is to provide for a fluid and streamlined inception and design phase followed by a rigorous test phase to ensure that all data meets the requirements for availability, integrity, and security.

Software development is a complex, iterative process in which SQA principles play an important role. This procedure does not provide a detailed implementation for all tasks associated with developing or maintaining DOE software. Rather it provides the framework for controlling, managing and documenting that process. The System Owner is responsible for including those elements of SQA applicable to the specific project.

## 8.0 PROCEDURE

Applications can cover a wide variety of data control and manipulation. They range from a simple application with a single table to support simple queries on a webpage to complicated multi-tabled databases containing sensitive data with intricate user interface. Application Development and Management is controlled through an eight phase process: Initiation, Application Definition, Development, Acceptance Testing and Baseline, Production, Revision and Maintenance, Annual Review, and Retirement.

- 8.1 Initiation – The initiation process is started when a perceived need for an application to accomplish a specific task or group of tasks is developed. This need is presented to the IRM staff and from there informal discussions formulate the concept and general scope of the proposed application. Once a concept has been formulated the ADIRM will determine if the proposed application is viable and if resources are available to pursue the development. Discussion at the management level will determine if the development will go forward and will align the project schedule with the priorities of the organization.
- 8.2 Application Definition – Once there is a general agreement among management to proceed, IRM will establish an APP. APPs are controlled as Technical Instructions Documents (TIDs) in accordance with Subject Area Description (SAD), Document Control, SAP-OD-410B-07, Control of Technical Instruction Documents. This project plan will define the overall objectives of the application; define the key roles of System Owner, Content Owner, Content Manager, and Developer; and provide the following information:
- 8.2.1 Statement of Need – The Statement of Need defines what need is being fulfilled by the application. It should also address the functionality of the system, who needs to access the system, how often, and where they are located. Also this section should discuss reporting requirements and any manipulation of data required. The generation of a flow chart that shows the flow of data is encouraged and may be required by the Developer to assist in application design. This section will be completed using information provided by the Content Owner and/or Manager.
- 8.2.2 Data Set – The data set is the entirety of the type of data that the application will be manipulating. This section will be completed using information provided by the Content Owner and/or Manager.
- 8.2.2.1 Data type - The data type should be described by description or title, approximate length, and whether it is a member of a subset of data.
- 8.2.2.2 Data Sensitivity – The data set shall also identify the sensitivity of the data in accordance with the EMCBC Policy on the Control of Unclassified Electronic Information, Legacy Procedure, PO-IRM-240-06. Attachment A has a summary chart from that policy.
- 8.2.2.3 Software Quality Assurance Checklists – The proposed purpose and functionality of the software is assessed to determine the need for a Software Quality Assurance Review utilizing the following forms; Checklists for Software Classification Determination, IMP-IRM-8308-03-F1, and Software Evaluation, IMP-IRM-8308-03-F2.
- 8.2.2.4 Records Management – Utilizing Attachment B “Is it a Record?” and IMP-IRM-8308-03-F3 as guidance, the Records Management Implications of the proposed application is determined.
- 8.2.3 Security Requirements – Once the Data Sensitivity has been established, the security and access requirements will be defined by the Developer and

documented in the APP. At a minimum, all applications are tested for SANS (SysAdmin, Audit, Network, and Security Institute) Top 20 Vulnerabilities (<http://www.sans.org/top20/>).

- 8.2.4 Development Schedule – The Developer will create a proposed schedule for completion with input from the ADIRM and Content Owner and/or Manager.
- 8.2.5 Life Cycle Analysis – This section will be completed by using the information provided by the Content Owner and/or Manager and it shall indicate a time frame for application retirement and final disposition.
- 8.2.6 Make or Buy Analysis - Once all of the above data elements are contained in the APP the System Owner or designee will conduct a Make or Buy analysis. This analysis should include Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), and the compatibility of other in-house applications or applications from other sites.
  - 8.2.6.1 Implementation - Once the analysis is complete, the System Owner or designee will determine how the application will be implemented. If purchased, the System Owner will oversee the procurement, and if by in-house development, the System Owner will establish the Data Base Management System and applicable user interface.
  - 8.2.6.2 Cost Estimate - Applications with a rough cost estimate of fewer than 80 hours of internal resources do not require a documented Make or Buy decision.
- 8.2.7 Approval – The ADIRM and the Independent Reviewer will approve the completed APP.
- 8.3 Development – The assigned Developer shall proceed with development, modification, or installation of the application. The Developer will work closely with the Content Manager to ensure that all the requirements of the APP are being implemented.
  - 8.3.1 Changes – During the course of all development phases there is a need for changes that were not anticipated during the original APP development. For the most part, changes are minor and do not affect the development requirements established in the APP. However, if there are any changes made that would affect the sensitivity of the data or the types and locations of users accessing the data, the APP will be updated to reflect the new needs and the Data Sensitivity and Security Requirements will be reexamined.
- 8.4 Acceptance Testing and Baseline – This phase has three distinct sub-phases: Alpha Testing, Beta Testing, and Conducting a Baseline. A Software Quality Assurance Review, when such a review is determined to be required by the Software Evaluation, IMP-IRM-8308-03-F2, is conducted as appropriate by the Independent Reviewer during this period. The complexity of the Software Quality Assurance

Review may be as simple as an independent review of the output or as complex as a detailed Software Quality Assurance Test Plan.

- 8.4.1 Alpha Testing is conducted once the Developer releases the application to the Content Manager and other applicable persons as determined by the Developer and Content Manager for initial testing. This may be done in whole or in part at the discretion of the Developer and the Content Manager. Alpha testing may be done in-house or from remote locations. However, ALL ALPHA TESTING IS CONDUCTED WITH INERT DATA. Real data is not to be used during alpha testing as it could very easily expose sensitive data. At the end of alpha testing the testers will develop a punch list for suggested changes or corrections. The Content Manager and Developer will then review the punch list and determine the path forward. Any major changes to the application will require a revision to the APP.
- 8.4.2 Beta Testing is conducted with live data. At the end of Beta Testing the testers will again develop a punch list of items that need correction. The Content Manager and Developer will then review the punch list and determine the path forward.
- 8.4.3 Any Software Quality Assurance Testing will be accomplished at this time in accordance with the APP or through the development of a Test Procedure Document (TPD).
- 8.4.4 A Baseline is conducted in accordance with IMP-IRM-8308-02, Configuration Management of Computer Systems and Networks. This process ensures that all cyber security controls are in place and functioning. Security Testing will be conducted in accordance with the applicable TIDs. Application specific security tests will be developed as needed and updated in the appropriate TID(s).
- 8.5 Production - Once all testing and security items have been resolved and with the concurrence of the Content Owner and System Owner, the application is considered to be certified and is placed into production and, if necessary, all code changes shall be checked into source control should a rollback be required.
- 8.6 Revision and Maintenance
  - 8.6.1 Minor changes may be made in accordance with the provision of Configuration Management of Computer Systems and Networks, IMP-IRM-8308-02, and **must** be documented in the IRM Project Management System under Application Support (WBS 1.4) as required by the Developer.
  - 8.6.2 Requests for major changes are required to be in writing, hard copy or electronic. Acceptable requests include, but are not limited to, email or a completed software change request form IMP-IRM-8308-03-F4.
  - 8.6.3 If a major revision (such as a change in data sensitivity, application access process, results of the Checklists for Software Classification Determination or Software Evaluation, or as deemed necessary by the

System Owner) to the application is required, the IRM Staff will develop an addendum to the existing APP to clearly define the needed changes and attach the addendum to the existing APP. The System Owner or designee will provide the necessary testing and baseline actions, including a Software Quality Assurance Review by an Independent Reviewer as appropriate, required to recertify the application for production.

- 8.7 Annual Review – Each application will be reviewed annually by the System Owner or designee to ensure that it is still needed and meets current security requirements. This review may be done in concert with other related applications. All reviews are documented in the IRM Project Management System, APP Log, and/or IM Maintenance Log as required.
- 8.8 Retirement – At the end of the life cycle the application will be retired in accordance with the APP and disposition will occur according to the IRM File Plan.

9.0 RECORDS MAINTENANCE

Records generated through implementation of this procedure are identified as follows and are maintained by the Office of Information Management in accordance with the EMCBC Organizational File Plan:

Records Category Code	Records Title	Responsible Organization	Quality Records Classification (Lifetime or Non-Permanent)
DAA-GRS-2013-0005-0007	System Development Records	OIRM	Non-Permanent
DAA-GRS-2013-0005-0004	Information Technology Operations and Maintenance Records	OIRM	Non-Permanent

9.1 References – Forms/Attachments/Exhibits

9.1.1 Forms

- IMP-IRM-8308-03-F1, Checklists for Software Classification Determination
- IMP-IRM-8308-03-F2, Software Evaluation
- IMP-IRM-8308-03-F3, Records Management Compliance Checklist
- IMP-IRM-8308-03-F4, Software Change Request

9.1.2 Attachments

- Attachment A - Summary Chart on Controls for Electronic Information
- Attachment B – Is It A Record?

**EMCBC RECORD OF REVISION**

Document Title: SOFTWARE APPLICATION DEVELOPMENT AND MANAGEMENT

If there are changes to the controlled document before the two-year review cycle, the revision number stays the same; one of the following will indicate the change:

I Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised, or

I Placing the words GENERAL REVISION at the beginning of the text. This statement is used when entire sections of the document are revised.

If changes and updates occur at the two-year review cycle, the revision number increases by one.

---

<b>Rev. No.</b>	<b>Description of Changes</b>	<b>Revision on Pages</b>	<b>Date</b>
0	Initial Information Management Procedure Supersedes IP-240-03, Rev. 2	Entire Document	08/30/12
1	Added requirements for Section 508 Compliance	Entire Document	08/05/15
	Added System Development Life-Cycle (SDLC) Management Requirement	Entire Document	
	Updated References	2	
	Updated format of 9.0 Record Maintenance	9	