Best IT Practices and Industry Standards for Automated Elections

Nelson J. Celis

Abstract:

Any computerized application system project, or simply an IT project, passes through the system development life cycle (SDLC) framework and the automated election system (AES) is not an exception. The SDLC framework provides a structured and standardized process for all phases of any computerized system development effort and such phases are project planning, requirements analysis, system design and development, system integration test certification, user acceptance test certification, system implementation/production, and system maintenance. Several industry standards are related to SDLC and these are the following:

1. ISO/IEC 12207/15288: Software/System Life Cycle Processes
2. ISO/IEC 20000 (IT Service Management) or ITIL (Information Technology Infrastructure Library)
3. ISO/IEC 27000: Information Security Management System
4. ISO/IEC 38500 (Corporate Governance of IT) or COBIT (Control Objectives for Information and related Technology)
5. ISO/IEC 29119 (Software Testing)
6. Voluntary Voting System Guidelines (VVSG). The VVSG are guidelines adopted by the United States Election Assistance Commission (EAC) for the certification of voting systems and these are very much applicable to the techno-legal provisions of RA9369. The VVSG is composed of two volumes: Volume I, Voting System Performance Guidelines and Volume II, National Certification Testing Guidelines.

The designated experienced project management team for future AES projects should adopt the above standards so as not to repeat the mistakes in automating the national and local electoral processes that the Country has been experiencing since 1996. More emphasis should be given on the 4^{th} and 5^{th} phases of SDLC where the project management team would clearly see the accuracy, reliability, auditability and security of all the system modules (i.e., counting, consolidation and canvassing, etc.) of the AES. On the part of the Commission on Elections, such adoption should be institutionalized to comply with RA 9369 and such could only be achieved through proper execution of its strategic information system plan.

Best IT Practices and Industry Standards for Automated Elections

Nelson J. Celis

I. THE SYSTEM DEVELOPMENT LIFE CYCLE

Any computerized application system project, or simply an IT project, passes through the system development life cycle (SDLC) framework (Figure 1) and the automated election system (AES) is not an exception. As indicated in the diagram, the SDLC framework provides a structured and standardized process for all phases of any computerized system development effort and such phases are:

1. Project Planning
2. Requirements & Specification Analysis
3. System Design and Development
    a. Architecture High Level Design
    b. Detailed Design
    c. Coding
4. System integration Test Certification
    a. Unit Testing
    b. Integration & Testing
5. User acceptance test certification
6. System implementation/production
7. System maintenance

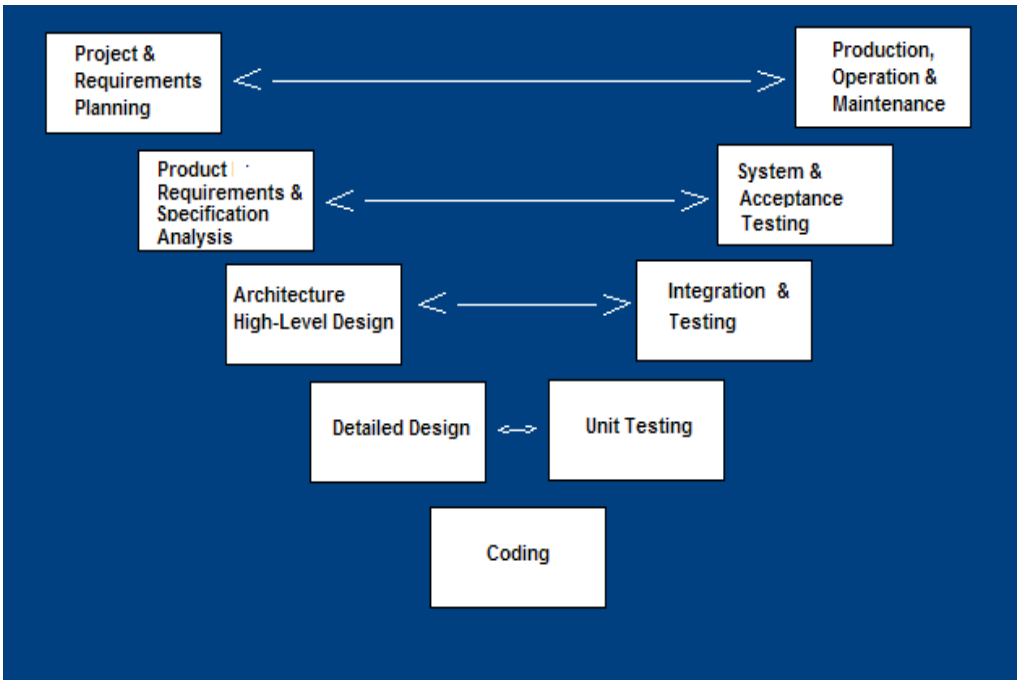

Figure 1. V-Shaped SDLC Model

In the past automation exercises, Phases 1 and 2 were done by Comelec with the technical help of the Advisory Council and stakeholders; Phase 3 had always been the responsibility of the winning bidder; Phases 4, 5 and 6 should have been the crucial job of the Comelec Advisory Council (CAC), Technical Evaluation Committee (TEC), and the winning bidder in the last elections; and Phase 7 has not been experienced in the past exercises especially that the AES used in the last elections was leased. Although it should be noted that an established international certification entity was tapped in the unit testing of the Precinct Count Optical Scan (PCOS) machines but with reservations on compensating controls.

Considering the V-Shaped SDLC model, the left side is focused on how should the AES work during elections and the right side is emphasizing the need to conduct test certifications. A case in point is the process of manufacturing a car. The SDLC model's left side can be compared with the design of the car that includes the engine power, the mechanical connections with the engine and the interior and exterior design while the SDLC's right side can be compared with the manufacturer's internal testing and test drives.

Among the SDLC phases, the most crucial phases in implementing any computerized application system are the 4th (i.e., system integration test certification) and 5th (i.e., user acceptance test certification) phases of the SDLC and this is related to RA 9369, Sec. 11:

> *"SEC. 11. Functions of the Technical Evaluation Committee. - The Committee shall certify, through an established international certification entity to be chosen by the Commission from the recommendations of the Advisory Council, not later than three months before the date of the electoral exercises, categorically stating that the AES, including its hardware and software components, is operating properly, securely, and accurately, in accordance with the provisions of this Act based, among others, on the following documented results:*
>
> 1. *The successful conduct of a field testing process followed by a mock election event in one or more cities/municipalities;*
> 2. *The successful completion of audit on the accuracy, functionally and security controls of the AES software;*
> 3. *The successful completion of a source code review;*
> 4. *A certification that the source code is kept in escrow with the Bangko Sentral ng Pilipinas;*
> 5. *A certification that the source code reviewed is one and the same as that used by the equipment; and*
> 6. *The development, provisioning, and operationalization of a continuity plan to cover risks to the AES at all points in the process such that a failure of elections, whether at voting, counting or consolidation, may be avoided.*

In the case of AES implementation, the above provision of the law refers merely to the following project milestones:

1. System Integration Test Certification. This is a certification process whereby the linking up of all the AES system modules, from the voting machine up to the national canvassing and consolidation system, through data communications facilities are evaluated for compliance based on pre-defined technical test procedures.
2. User Acceptance Test Certification. This is a certification process whereby the AES is evaluated using test scripts vis-a-vis requirements defined in the Terms of Reference.

The 6th phase, the system implementation or the production mode, is the actual use of the AES and it should conform with the blueprint of the overall project plan, requirements and specifications as defined in Phases 1 and 2.

II. INDUSTRY STANDARDS

There are several industry standards based on best practices that could be adopted in implementing an AES and these are the following:

- ISO/IEC 12207/15288: Software/System Life Cycle Processes
- ISO/IEC 20000 (IT Service Management) or ITIL (Information Technology Infrastructure Library)
- ISO/IEC 27000: Information Security Management System
- ISO/IEC 38500 (Corporate Governance of IT) or COBIT (Control Objectives for Information and related Technology)
- ISO/IEC 29119 (Software Testing)
- The Voluntary Voting System Guidelines (VVSG). The VVSG are guidelines adopted by the United States Election Assistance Commission (EAC) for the certification of voting systems and these are very much applicable to the techno-legal provisions of RA9369. The VVSG is composed of two volumes: Volume I, Voting System Performance Guidelines and Volume II, National Certification Testing Guidelines.

Each industry standard could fit in any project management milestones of the AES project execution. The good thing about the VVSG is that it is tailored fit for automated election systems and it has incorporated most of the ISO framework concepts. Nonetheless, the control objectives of the ISO 27000, COBIT/ISO 28500 and ITIL/ISO20000 could even enhance the VVSG to beef up the support and engagement of major AES stakeholders.

Based on the VVSG manual, hereunder are the key points explained therein:

> *"The purpose of the Voluntary Voting System Guidelines is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic*

functionality, accessibility and security capabilities required to ensure the integrity of voting systems. The VVSG specifies the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems.

Volume I, the Voting System Performance Guidelines, describes the requirements for the electronic components of voting systems. It is intended for use by the broadest audience, including voting system developers, manufacturers and suppliers; voting system testing labs; state organizations that certify systems prior to procurement; state and local election officials who procure and deploy voting systems; and public interest organizations that have an interest in voting systems and voting system standards.

The Volume I describes the following:

- *Functional capabilities required of voting systems*
- *The new standards that make voting systems more usable and accessible for as many eligible citizens as possible*
- *Specific performance standards for election system hardware, software, telecommunications, and security, voting system security requirements and includes new requirements for voting system software distribution, generation of software reference information, validation of software during system setup, and the use of wireless.*
- *Requirements for vendor quality assurance and configuration management practices and the documentation about these practices required for the certification process.*

Volume II, the National Certification Testing Guidelines, is a complementary document to Volume I. Volume II provides an overview and specific detail of the national certification testing process, which is performed by independent voting system test labs accredited by the EAC. It is intended principally for use by vendors: test labs: and election officials who certify, procure, and accept voting systems."

The Volume II describes the following:

- *Description of the Technical Data Package that vendors are required to submit with their system for certification testing*
- *The basic functionality testing requirements*
- *Requirements for hardware, software and system integration testing*
- *Requirements for usability and accessibility testing*
- *Requirements for examination of vendor quality assurance and configuration management practices.*

III. AES IMPLEMENTATION FRAMEWORK

The above six (6) industry standards are very much applicable to Philippine setting and it is matter of properly carrying out the project management implementation. In this regard, the inclusion of the industry standards within the premises of a successful AES project completion is simplified by the author in Figure 2.

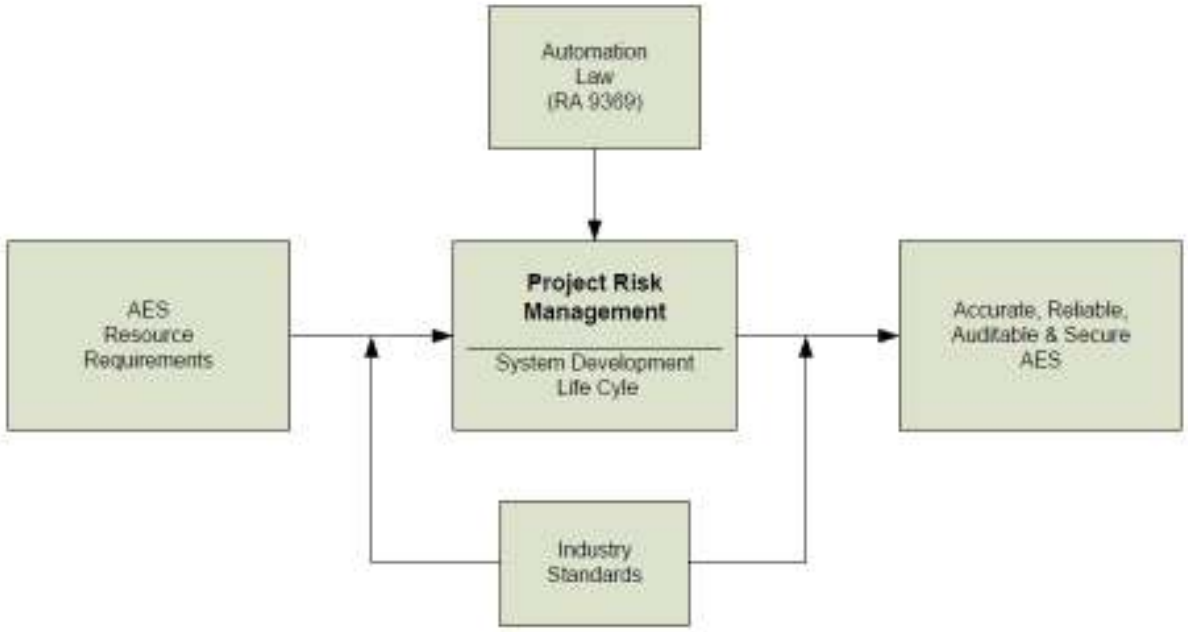

Figure 2. AES Implementation Framework

The AES Implementation framework is clearly giving us an idea that:

- The project risk management (PRM) of the SDLC positively influences the accurate, reliable, auditable and secure AES.
- The industry standards positively moderate the influence of PRM on the accuracy, reliability, auditability and security of AES.
- The full utilization of AES resource requirements in the SDLC is moderated by the conformance of the PRM team with the industry standards' control objectives.
- The systems development of the AES would only be successful if all the provisions of the automation law are strictly complied with.

IV. LEADERSHIP AND MANAGEMENT IN THE FRAMEWORK

As defined in RA 9369, Figure 3 shows the responsible organizations in implementing the AES and their respective leaders are expected to perform good governance with the end in mind of ensuring free, orderly, honest, peaceful, credible and informed elections. Still, there's no other person than the Comelec Chairman who would direct the AES project in accomplishing it successfully. It's his leadership knowledge and skills that would carry out the AES implementation framework with the help of the Advisory Council, Technical Evaluation Committee and subject matter experts. Getting things done in compliance with the automation law is of utmost importance for the Comelec Chairman. He should not only be a professional lawyer but also a good manager.

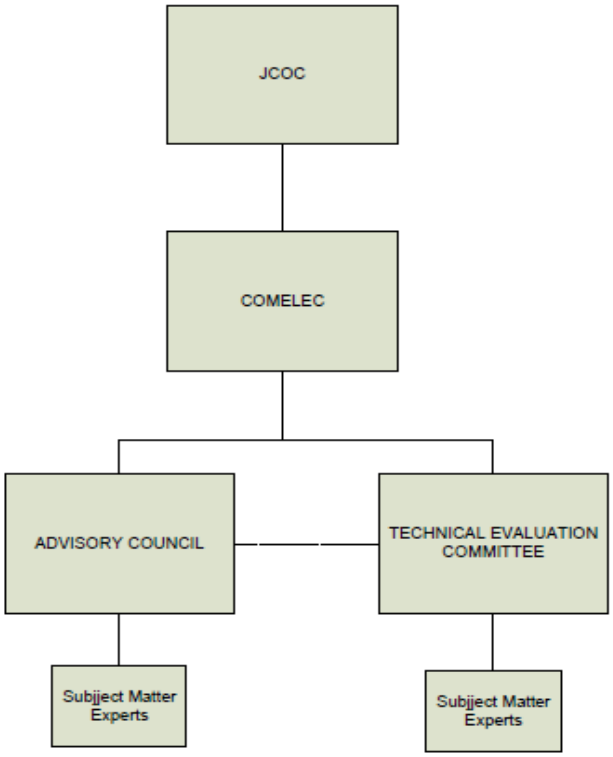

Figure 3 – Responsible organizations in AES implementation

The subject matter experts are stipulated in Sections 8 and 11. These are resource persons that the CAC and TEC could have tapped in the last elections in helping them out with the project risk management, specifically with the time pressure then. They are the IT experts and auditors from private and government organizations who have experienced finishing similar magnitude of project undertakings. Serving as project consultants, their value would be in risks mitigation, problem troubleshooting and in SDLC planning and controlling of the 4th and 5th phases of the AES project. Besides, the designated managers and members of the CAC and TEC have other full time jobs in their respective organizations and the possibility of overlooking major decisions and even hardly visible activity but critical is a big probability.

The Joint Congressional Oversight Committee (JCOC) has to actively play in the AES Implementation Framework to monitor and evaluate the implementation of election automation law. Since their function is oversight in nature, they could come in the 5th phase of the SDLC just to make sure that all the techno-legal provisions of the law are carried out in the user acceptance test certification. But of course, it is much appreciated by the electorates if JCOC would do a comprehensive post-election review and evaluation of the AES and make appropriate recommendations to soonest possible time.

Hereunder are the major functions of the above organizations:

- Advisory Council, RA 9369, Sec. 9:
  - Recommend the most appropriate, secure, applicable and cost-effective technology to be applied in the AES
  - Provide advice and assistance in the review of the systems planning, inception, development, testing, operationalization, and evaluation stages
  - Provide advice and/or assistance in the identification, assessment and resolution of systems problems or inadequacies
  - Provide advice and/or assistance in the risk management of the AES especially when a contingency or disaster situation arises.
  - Prepare and submit a written report, which shall be submitted within six months from the date of the election to the oversight committee, evaluating the use of the AES.

- Advisory Council, RA9369, Sec. 8:

  "The council may avail itself of the expertise and services of resource persons who are known independence, competence and probity, are nonpartisan, and do not posses any of the disqualifications applicable to a member of the Advisory Council as provided herein. The resource persons shall also be subject to the same prohibitions and penalties as the members of the Advisory Council."

- Functions of the TEC are described on page 3.

  As also stipulated in RA 9369, Sec. 11:

  "The Committee (TEC) may avail itself of the expertise and service of resource persons who are of known independence, competence and probity, are no partisan, and who do not possess any of the disqualification applicable to a member of the Advisory Council as provided herein. The resource persons shall also be subject to the same prohibitions and penalties as the members of the Advisory Council."

- JCOC, RA 9369, Sec. 33.

  "SEC. 33. Joint Congressional Oversight Committee. - An Oversight Committee is hereby created composed of seven members each from the Senate and the House of Representatives, four of whom shall come from the majority and three from the minority, to monitor and evaluate the implementation of this Act. A written report to the Senate and the House of Representatives shall be submitted by the Advisory Council within six months from the date of election. The

oversight committee shall conduct a mandatory review of this Act every twelve (12) months from the date of the last regular national or local elections."

"The oversight committee shall conduct a comprehensive assessment and evaluation of the performance of the different AES technologies implemented and shall make appropriate recommendations to Congress, in session assembled, specifically including the following:

1. *An assessment and comparison of each of the AES technologies utilized, including their strengths, weakness, applicability or inapplicability in specific areas and situations;*
2. *An evaluation of their accuracy through a comparison of a random sample of the AES election results with a manual tabulation, and the conduct of similar tests;*
3. *As to the scope of AES implementation in the subsequent elections, provide for recommendations x x x*
4. *As to the kind of AES technology, provide for proposals as to whether:*
    a) *A particular AES technology should no longer be utilized for being obsolete, inapplicable, inaccurate or with a defect which cannot be remedied;*
    b) *An enhancement or improvement is needed to an AES technology x x x*
    c) *A particular AES technology is already appropriate and should be utilized fully for subsequent election; or*
    d) *The testing or adoption of new technologies which may have emerged x x x*

V. RECOMMENDATIONS

To ensure free, orderly, honest, peaceful, credible and informed elections, the author is recommending the following:

- Adopt the AES Implementation Framework using VVSG combined with other ISO industry standards for the next elections starting in 2013
- Raise up the leadership/management knowledge and skills of the main players in the AES project implementation to comply with the election automation law
- Beef up the certification processes in the 4th and 5th phases of SDLC by tapping subject matter experts and involving professional auditing firms and the Commission on Audit.
- JCOC to intervene in the 5th phase of the SDLC to ensure that the user acceptance certification test is properly executed and audited

VI. CONCLUSION

Banking corporations, whether private or government-owned, have the most complicated banking application systems compared with any economic industries. Their systems are even more complicated than AES. And why do these banks have to implement these systems on time and within budget? It's obvious because they're after their competitiveness within the banking industry and always looking ahead of their bottom-lines. To top it all, it is very much critical in handling their depositors' money as any single error would mean catastrophic repercussions to the point of business closure. But the most important to these bankers is that they follow best practices and industry standards in handling IT projects under the strict leadership and management of their respective CEOs. In fact, they even collaborate to one another when introducing new products and services within the ATM network consortia without affecting the profitability of their respective banks. If these banks could manage such enormous IT projects, the author believes that it could also be done by our legislators and officials of the COMELEC.