Auditing the Software Development Lifecycle
ISACA Geek Week

Mike Van Stone
Sekou Kamara
August 2014
Introduction
  - Audit Scope
  - Project Initiation
  - SDLC Processes
  - Stakeholders
  - Common Development Methodologies
Auditing the Software Development Lifecycle
Other Key Topics
  - ERP Application Controls
  - Secure Development
Audit Scope

- Project Governance
- IT Controls
- Financial Controls
Project Initiation
Key Considerations

- Is the project aligned with the company’s strategy?
- Are there adequate supporting artifacts?
  - Strategic plan
  - Business case or scoping document (features)
  - Project charter
  - Executive sponsorship
SDLC Processes

- Process Overviews
  - Project Initiation
  - Governance
  - Functional and Technical Requirements
  - Coding

- Process Overviews
  - Quality Assurance
  - Rollout Plan
  - Product Readiness
  - Implementation
  - Support
SDLC Stakeholders

- Senior Leadership Team
- Product Management
- Development
- Quality Assurance
- Compliance/Legal
- Information Security
- Chief Technology Office
- Project (or Program) Management Office
- Accounting/Finance
- Sales
- Services
- Training
- Support
- Data Center
- Customer
- Operations
Common Development Methodologies

Waterfall
- Requirements
- Design
- Implementation
- Verification
- Maintenance

Iterative
- Product Backlog
- Sprint Backlog
- Sprint
- Working increment of the software
Auditing the Software Development Lifecycle
Governance

Key Considerations

- Are the project management policies, procedures, and standards complete and up-to-date?
  - Development, maintenance, and monitoring
  - Common tools and training on tools
- How effective is the project planning and management oversight?
  - Stakeholder engagement
  - Risk and issue management
  - Resource management
  - Inter-dependencies and ongoing communications
  - Scope change controls
  - Project closure and hands-off
Project Planning
Key Considerations

- Are estimates based on complexity and completeness of required activities?
- Is the team considering other dependencies when prioritizing key tasks?
- Does the plan highlight critical path versus critical activities?
- How are inter-dependent project plans synchronized and maintained?
- Are key task owners identified in the project plan?
- Do major milestones align with the business case?
- Has the project plan been formalized, reviewed, and approved by the project sponsor?
Risk & Issue Management
Key Considerations

- Have issue documentation and prioritization standards been established?
- Is the risk and issue register periodically reviewed?
- Are risks and issues escalated to appropriate level of management per the issue and risk management policy?
- Do the issue management standards distinguish between risks and issues?
- Is there a process to promote the sharing of knowledge of workarounds and lessons learned?
- Is there a standard issue management tool with appropriate access controls?
- Does the project team audit the risk and issue register against project management standards?
Resource Management
Key Considerations

- Is there a complete integrated enterprise resource plan?
- Are resource model assumptions documented and significant changes revalidated?
- Can the resource plan requirements align with the business case and financial forecasts?
- Is there an up-to-date resource availability calendar?
- Has the availability of shared resources been evaluated?
- Can the project plan highlight resource shortages in the enterprise resource management plan?
Ongoing Communication
Key Considerations

- Is the communication plan designed to inform both technical (IT) and non-technical (business) personnel?
- Is the communication effort focused on:
  - Promoting dialogue between project teams (regular team update)?
  - Creating awareness about the progress, risks, and issues?
  - Building cooperative environment?
  - Managing and preventing conflict?
  - Getting stakeholders input and maintaining executive commitment?
  - Communicating and addressing risks and issues as soon as they are identified?
- Has the plan been documented and assigned an owner?
- Effective communication involves more than the periodic status deck
Scope Change Controls

Key Considerations

- Are all change requests submitted in writing and/or are all changes traceable?
- How is the project manager ensuring that everyone (requester, reviewer, approver, and implementer) follows the change control process?
- Is there an exception procedure for emergency changes?
- Are approvals obtained after an impact analysis?
- The goal is to minimize change impact through communication and coordination.
Functional and Technical Requirements
Key Considerations

- Have business requirements been adequately documented and vetted with process owners, analysts, and end users?
- Can the requirements be traced to business case objectives?
- Are there standards for documenting requirements?
- Have implementation requirements been considered?
- Is the design team considering key technical criteria such as: compatibility, extensibility, fault-tolerance, maintainability, and integration?
- Do the requirements include security and regulatory compliance?
- Has the architectural team provided visibility to the technology platform and strategies?
Coding Key Considerations

- Is the process designed to support the development workflow?
- Has a policy been implemented to facilitate environment planning, prioritization, and security?
- Has the team established peer code review process?
- Are automated testing scans performed against coding standards?
- What controls are in place to ensure adequate version control, code review, and code promotion?
- Is there a policy governing the use of open source code?
Quality Assurance
Key Considerations

- Have quality requirements been defined including how to measure them?
- Are coding and naming standards included in quality control requirements?
- Does the project plan include steps for testing quality before a quality assurance validation?
- Does the project team include an independent quality assurance function?
- Is there a follow-up point to ensure quality between project phases?
- Is there an exception handling process?
Rollout Plan
Key Considerations

- Did the team include the transition/rollout activities in the project plan with due dates/owners?
- Did the plan include testing to ensure the product will meet all requirements in full production?
- Has the team finalized all documentation including user and technical training material?
- Are the help desk and operations teams ready to support users and the system without relying on the project team?
- Was the rollout schedule coordinated with user training?
- Does the project plan include steps to formally close the project and obtain all sign-offs?
Product Readiness
Key Considerations

- Is there a product general availability approval process evidenced by supporting documentation?
- Key criteria include:
  - Customer testing (pilot)
  - Patch management plan
  - Minimum quality/defect requirements
    - Exceptions and follow-up plans
Implementation Key Considerations

- Is there a detailed implementation plan with major milestones?
- Did the planning include coordination with development and support?
- Is the implementation schedule aligned with customer readiness and other priorities?
- Is there an effective implementation issue management process including triage and escalation of issues?
- Does the process include knowledge sharing among various teams?
- Have the go/no-go criteria been defined and approved by management?
- Is there a tested back-out plan?
- Is the transition plan approved by both implementation and support?
- What are the sign-offs requirements?
Transition to Support
Key Considerations

Customer Performance Issue

TIER 1 SUPPORT (FRONT LINE)

TIER 2 SUPPORT

MANAGEMENT  TIER 3 R&D
Other Key Topics
Financial Controls
Key Considerations

- How are project expenses tracked against approved business case?
- Are revisions to the business case approved by the right level of management?
- Is time accurately tracked and managed against budgets?
- Is vendor performance aligned with spending to date?
- Is the software capitalization impairment analysis completed and documented?
- Is there a formalized process for revenue recognition and capitalization journal entry review?
- Is there a product pricing review board?
ERP Controls
Key Considerations

- Is there an access and segregation of duties design matrix?
- Have automated accounting instructions been assessed?
  - Intercompany eliminations?
  - Transaction mapping?
  - Account rollups?
- Are there adequate supporting documents for the design and controls for:
  - Interfaces?
  - Job scheduling?
  - Report design?
  - Application controls and integrity reporting?
- Are policies, procedures, and process flows kept to date?
Appendix
Product Development Security Framework

Key Considerations

- Security training
- Security requirements in design
- Threat modeling
- Design reviews
- Quality assurance testing
- Access reviews
- General availability (and interim gating)
- Incident response planning