Architecture Maturity: The PDCA Cycle

The architecture maturity cycle is based on the well recognized *Plan-Do-Check-Act* cycle, a four phase cycle for implementing change. Refer to Figure 11.1-1. Repetition of the PDCA cycle results in the continuous improvement and growing maturity of the architectural description.
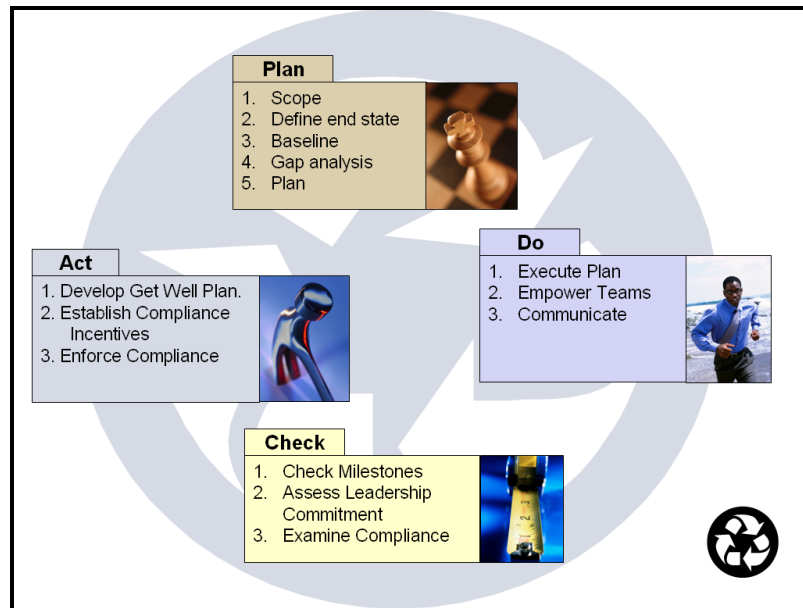

Figure 11.1-1: PDCA Cycle

The cycle can also be used to organize and conduct the *governance* of an architecture development effort, as described below:

11.1.2   PLAN

11.1.2.1   Decide Scope. The first step in planning is to decide the *scope* of governance. To do this, answer five questions:

1. How many Governance Teams are required? For example, you may feel the need to establish an Architecture Investment Team and a Technical Team to govern your architecture description.
2. What decisions will each of the Governance Teams make?
3. Who is accountable to the Governance Teams? Lay down lines of authority/responsibility.
4. What governance policies are needed? Such policies authorize the governance teams to make decisions on behalf of the architecture Sponsor.
5. What are the most important goals of governance in your case (e.g., to make cost-effective use of technology[1], alignment of the architectural description with larger strategic goals, the efficient use of technology assets , or reduction in programmatic risk)?

---

[1] Governance contents adopted from the U.S. Department of Justice, Office of Justice Programs

11.1.2.2   Determine Type of Governance. Decide what type of governance model your organization needs (or, more realistically, CAN ACHIEVE given the level of cultural resistance that is typical of an organization being asked to change the way it does business). There are nominally three models of governance: *Centralized*, *De-centralized*, and *Hybrid*.[2]   Table 11.1.2.2-1 compares these three governance models.

Table 11.1.2.2-1 – Governance Models

Governance Models			
	Centralized	**Hybrid**	**Decentralized**
FOCUSES ON…	Cost	Asset Utilization	User requirements
CHARACTERISTICS	Strong governance	Less robust governance	"Governance-lite"
TYPICAL SOLUTIONS	Low -cost, low risk, highly standardized	Mix of enterprise and locally optimized solutions	Solutions focused on local requirements

Centralized governance is characterized by attentive, central control over all aspects of technology decision making -- including investment, policy, and standards. To be a success, it requires the highest levels of leadership support, comprehensive policy formulation, and the diligent enforcement of compliance. Centralized governance focuses on cost-effectiveness, usually attempting to leverage the "centralizing" authority's wide span of control to lower costs by means of standardization. Its policies and processes support rigid technology standards and enthusiastic compliance enforcement. The goal is a low-cost, low-risk, highly standardized enterprise – however, one neither designed to be highly responsive to localized requirements.

Decentralized governance is characterized by less robust control. To be effective, this governance model requires the highest levels of communication, collaboration and coordination. Decentralized governance focuses on innovation and autonomy to allow for locally-optimized technology solutions. Few if any enterprise-wide technology or business process standards are recognized. Relatively few formal governance mechanisms are required – instead, local requirements govern technology investment. The result is technology that is highly responsive to local requirements, but having little enterprise-wide standardization.

Hybrid governance tries to balance the two other models. It strives for sharing and re-using processes, systems, technology and data, but without draconian enforcement, in the realization that some localized solutions may indeed be necessary and/or are not worth the effort to share. Hybrid governance teams

---

[2] <u>IT Governance on One Page</u> by Peter Weill and Jeanne W. Ross. Center for Information System Research. Sloan School of Management. November 2004. CISR WP No. 349.

stay busy persuading or otherwise dealing with those who do not wish to leverage the enterprise solutions. This model results in a high utilization of technology assets, but allows for a mix of localized and enterprise-wide solutions.

11.1.2.3   Baseline Current Governance. Survey your organization's existing governance mechanisms to determine its level of governance maturity. Mechanisms include governance teams, governance policy, documented processes, and compliance rules. You might discover you have virtually no existing governance mechanisms to build upon.

11.1.2.4   Analyze Gaps. Perform a gap analysis between the baseline and your desired level of governance maturity. Determine how much support from leadership you will need to overcome the inherent and inevitable resistance to change within the organization. Without strong and consistent leadership support, moving to the maturity level you desire may be impossible.

11.1.2.5   Create Transition Plan. Based upon the results of the gap analysis, develop a plan to reach your desired governance model. The plan can be as simple as a Plan of Action and Milestones (POAM) or as complete as a GANTT chart with full resources allocations depicted. NOTE: The plan should avoid the high-risk "Big Bang" approach to the advance of governance – wherein all governance improvements are rolled-out on a single date -- and aim instead to build toward the desired maturity in stages. Refer to Figure 11.1.2.5-1.
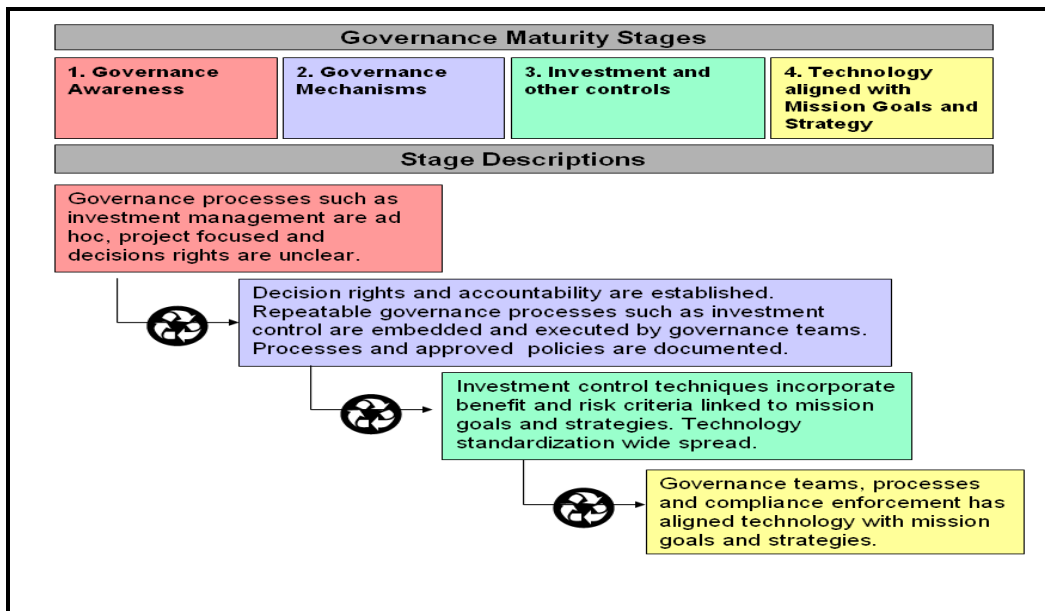

Figure 11.1.2.5-1: Governance Maturity Model

Much like spiral development, the gradual implementation of architecture governance is a low-risk approach. It lets you "build" a little governance at a time, field the first installment quickly, and learn a lot in during the process.

11.1.3 DO

11.1.3.1 Begin Execution. Time to execute the plan, monitor, and manage. One of the earliest steps for any major project is to hold a kickoff meeting with your team and stakeholders. Be sure your message is well- crafted and has already been adequately socialized. Consider hosting the meeting using web collaboration tools such as Webex or NetMeeting.

To prepare for your kickoff meeting, you should have the following ready to present:

- Governance Goals, Teams and Decision Rights
- Organization Chart
- Responsibilities Matrix
- Schedule of Staff Meetings, Product Reviews and Maturity Milestones

During execution you will need to monitor milestones, costs, quality, risks and performance and be prepared to generate "Get Well" or risk mitigation plans.

11.1.3.2 Empower the Governance Bodies. Critical to establishing governance is empowering the governance teams with *decision rights*. Without this step you will end up with teams that are advisory bodies only, and powerless to make decisions. Teams having responsibility *but insufficient authority* are not governance teams.

Decision rights need to be clear, concise, documented and communicated. The processes that describe how the governance teams receive information, how they interact with each other and other organizations needs to be similarly documented, well communicated and supported by policies.

11.1.3.3 Communicate. Frequent, effective communication is essential to governance success. Governance policies and processes need to be clearly communicated to stakeholders often and in various ways. Email by itself is no longer a sufficient means of communication.

The Communications Plan should address the details of a communication campaign that *times* the release of governance directives, training, posters, etc. Governance implementation will have to compete with a score of other projects that generate emails, IMs, memoranda, blog entries, etc. You need to get your message out there and heard above the noise. Getting people motivated to work on your project, respond to governance data calls, etc., requires communication that is clear, concise, and persuasive.

11.1.4 CHECK

11.1.4.1 Check Milestones, Quality and Risks. The next task is to monitor compliance with the chosen governance regime and enforce it when necessary. Your Quality Management Plan should have described what governance artifacts should be inspected, and upon what criteria they are evaluated. For example, Governance Team charters or decision rights policies should be reviewed for sufficiency. They should then be inspected to see how/if they were disseminated to stakeholders.

Your Risk Management Plan should describe how to identify and prioritize risks based on both quantitative and qualitative analysis. The plan should also address the creation of mitigation plans for the most urgent and/or higher-impact risks. Risk mitigation plans need to be tracked through completion like any other task.

11.1.4.2 Sustain Leadership Commitment. Leadership commitment is critical to the success of any projects that affect an organization as fundamentally as do governance, IT Portfolio Management, or Enterprise Architecture. Executive leadership is required to deal with such issues as organizational parochialism, cultural resistance to change, and fluctuations in resource availability. Executive leadership can also support the achievement of governance maturity by resourcing it adequately and promoting better information sharing.

When executive leadership or senior management ignores its governance responsibilities, there are consequences. Table 11.1.4.2-1 shows examples of those consequences.[3]

Table 11.1.4.2-1: Consequences of No Leadership Commitment

Consequences of No Leadership Commitment	
Leadership Fails To…	**Consequences**
Set Technology Budgets	Despite high spending, the organization does not develop a technology solution that furthers its strategy.
Prioritize Business Processes	Lack of focus results in all technology projects being treated as if they were of equal importance. The supporting technology units (e.g., IT Development), becomes overwhelmed trying to support scores of projects instead of focusing on those that have enterprise-wide value.
Set Realistic Security Policies	Unnecessary security or privacy controls may inconvenience customers, employees and suppliers. Conversely, an under-emphasis on security can make the organization's data critically vulnerable.

11.1.4.3 Determine Degree of Compliance. Obstacles to 100% compliance with a governance regime may include too many regulations at all levels (national, international, DoD, Service/Agency, and Command requirements), increased complexity of the enterprise itself, or partial organizational disruption due to the incomplete adoption of an emerging technology or other ongoing organizational shifts.

---

[3] SOA Governance, PowerPoint Briefing, IBM 2006.

11.1.5   ACT

11.1.5.1   Develop Get-Well Plan. For governance problems that have not already been mitigated through risk management, a Get Well Plan needs to be developed and "sold" to senior management. The Get Well Plan might include such proposed remedies as a call for more resources, delay of a schedule milestone, or personal intervention with the head of an uncooperative department.

11.1.5.2   Establish Compliance Incentives. Compliance should be rewarded and non-compliance punished. Positive steps toward the enforcement of governance include the granting of compliance awards by senior management, articles in organizational newsletters, bonuses, and letters of commendation.

11.1.5.3   Enforce Compliance. Your Quality Assurance Plan should describe how stakeholders' compliance with published governance policies and processes will be monitored. When compliance issues are found, they need to be documented and shared with the management team of the non-compliant stakeholder. A Performance Improvement Plan (or equivalent, less formal corrective action) should be written up collaboratively and then monitored. Should non-compliance continue bring the issues, documentation and alternative solutions to the attention of executive leadership.