APPLYING THE CPR FRAMEWORK TO IT GOVERNANCE

David Pultorak: In conjunction with Harris Kern's Enterprise Computing Institute

The Conformance, Performance, and relating Responsibility (CPR) Framework is a means to more accurately model corporate governance in today's multi-dimensional business environment. It defines governance as a systematic pattern of the board, management, and staff of a corporation that is directed towards the corporation achieving sustainable financial results. This behavior must be directed towards the four primary assets of the business, namely: infrastructure, clients and external stakeholders, internal people and process, and value creation. Effort is directed in three dimensions:

- Conformance to legal and regulatory requirements, from SEC and IRS to SOX, HIPAA, quality certifications, and even codes of ethics

- Performance, financial and otherwise such as client satisfaction, employee productivity, and business processes

- Relating Responsibility to maintain rapport with all relevant stakeholders, such as providing transparent and timely information on the corporate health

This same CPR Framework can be applied to IT governance, which is a necessary subset of any good corporate governance methodology. Applying the CPR Framework to IT governance can be done using the following guidelines:

- The Board, not the IT function, must be the prime driver for IT governance, in order to achieve the common interface and channel for governance needed throughout the corporation.

  o Where IT really matters to the corporation's future, it makes sense to involve corporate directors in infrastructure concerns. The CIO, on the other hand, should help influence the decision of the Board in determining the different roles with respect to IT governance in the performance, conformance, and relating responsibility aspects.

  o The CIO should also leverage Service Level Management as the "communications interface" between corporate and IT governance. It is advisable to adopt and adapt internationally recognized standards understood by IT, the defacto standard for which is the IT Information Library (ITIL). ITIL is strong in the areas of Performance and Relating Responsibility, but is weak in Conformance aspects. To cover these, one should look into the internationally recognized guidance contained in CobiT which focuses on control and compliance.

- Sustained financial results must be the objective and prime driver for IT decisions and actions.

  o All day-to-day decisions and actions must include a focus on and consideration of sustained financial results as a goal. Go / no-go decision on an IT change should not be made just on technical merits; the business impact of the change must be considered as well. The IT Information Library's process guidance for Service Level Management and Financial

Management for IT Services are recommended sources of knowledge on how to make this happen.

- The four primary assets of a business mentioned at the start of the article must be governed along the three CPR dimensions consistently.

  o A dashboard of metrics required to manage the current state of the IT function and its future state should be developed, similar to this:

Asset Areas ▶		Infrastructure		Clients & External Stakeholders		Internal People & Process		Value Creation	
Governance Dimensions▼	*State*▶	Current	Future	Current	Future	Current	Future	Current	Future
Conformance									
Performance									
Relating Responsibly									

- Emphasis must be on changing behavior, rather than introducing or changing work artifacts; roles must be set out, including expected behavior changes

  o Each internal key stakeholder must have his or her activities relative to IT governance stated as a set of job parts and standards (completing the statement "performance is effective when…"). The 4-S technique of job planning (understanding the Services, Stakeholders, Standards, and SMART goals) is one effective technique for doing this. This same approach can be done in determining the roles and responsibilities of the clients and external stakeholders.

- Other IT governance activities (such as IT Service Continuity Management) and frameworks (such as the IT Infrastructure Library) must be aligned within the CPR framework.

  o IT Information Library (ITIL) provides guidance and mechanisms that are ideal for realizing the Performance and Relating Responsibility dimensions of IT governance. It also enables conformance by specifying the process domains required to carry out the business of IT, which is a necessary basis for ensuring compliance with codes produced by relevant authorities. The service focus proposed by ITIL allows the board to expect more, demand more, and to require greater transparency in reporting on the business value of IT services.

  o Control Objectives for Information and Related Technology (CobiT) framework focuses on compliance and control. The guidance comes from the perspective of IT auditors, and it substantially strengthens the EDP audit function. It is detailed, prescriptive, and complete, and provides a standardized approach to IT accountability. CobiT is ideal for approaching the Conformance dimension of IT governance, and is in fact applicable beyond this dimension, with guidance in seven critical areas: effectiveness, efficiency, availability, integrity, confidentiality, reliability, and compliance.

- The Capability Maturity Model (CMM) and the later integrated version (CMMI) were created to optimize software development through a framework of continuous process improvement, defining five levels of maturity of software processes. A framework for assessment that is compatible with CMMI is the ISO/IEC 15504. Both of these can be integrated into the CPR governance framework primarily within the Performance dimension. Tracking of compliance to specified policies and procedures falls under the Conformance dimension, and managing perceptions around capability achievement falls under the "Relating Responsibility" dimension.

As can be seen from the above discussion, IT governance really involves a change of behavior in everyone in order for it to have an effective, long-term benefit to the financial sustainability of the business. It is not about passing some audit or test, documenting processes, or measuring everything that can be measured – but rather it is all about re-orienting everyone's frame-of-mind towards what is essential to the business.