Operational IT governance

Murray Cantor
John D. Sanders

May 15, 2007

This article introduces an operational approach to IT governance, describing governance as an intentional activity with its own lifecycle and artifacts. The authors then describes a value-based approach to IT governance processes and a set of principles that IT organizations can adapt to realize the benefits of governance in their business setting.

In this paper we focus on two applications of IT governance:

- Governance of IT processes such as those found in the Information Technology Infrastructure Library (ITIL) or Control Objectives for Information and related Technology (CobiT) standards
- Governance of business processes supported by IT

Governance at its essence is about decision-making and communications. The need for good governance stems from the need of organizations to make good decisions and communicate them effectively. Often, when faced with poor outcomes, the organization needs to review how the decisions were made and put in place structures that support better decisions going forward. These decisions can be large, such as whether to invest in a new initiative or approve an annual report; or the decision can be routine, such as whether to provide access to sensitive data or include software code in a release.

As IT has matured, the emergence of service orientation and Service Oriented Architecture (SOA) has presented a new set of governance challenges. The modularity and efficiencies enabled by service orientation provide the means to do both good and harm more quickly. The agility of SOA requires an organization to be more deliberate in its decision-making, a capability that is perhaps the true benefit of effective governance. Organizations adopting SOA need not only apply governance to the service artifact lifecycle processes, but also need to consider the impact of SOA on all IT governance sub-disciplines, such as portfolio governance or data governance. This resetting of IT governance for IT organizations adopting SOA is called SOA governance.

The emergence of governance on the IT landscape

IBM clients are increasingly focused on IT governance for two key reasons:

- The need to meet and document compliance to externally imposed business practices, including:
• Corporate and industry regulations and related compliance requirements such as Sarbanes-Oxley, the Health Insurance Portability and Accountability (HIPPA), the Payment Card Industry Data Security Standard (PCI DSS), Basel-II, and others
• Corporate policies such as financial controls and human resources
• Participation in broader organization business processes
• The desire to deliver more value to the business from the IT operations and investments. For example:
  • The need for business-critical systems to be available when the business or consumer requires them
  • Assuring the IT operations support and do not hinder evolving business strategies
  • Minimizing costs while delivering needed services
  • The desire to receive value from and mitigate risk of the adoption of SOA
• The desire to improve the agility, value, and innovative capabilities of their development organization; e.g., new product development, software development, new service creation

In this paper, we describe an operational approach to IT governance which provides a process for addressing the broad picture of IT governance given in Figure 1 (courtesy of Avi Yaeli and Clay Williams, IBM Research). The IT governance process has its own set of artifacts and a recurring lifecycle. The governance process lifecycle includes capturing the governance needs of an organization and creating, deploying, and evolving a governance solution that meets those needs while proactively balancing value and risk.

Figure 1: The relationship of governance, management, and business concerns

Adopting operational governance offers a practical approach for organizations to provide the fundamental value they are trying to deliver, whether that is organizational efficiency, customer intimacy, or product innovation.

We conclude this paper with a set of principles for effectively applying IT governance.
Defining governance

There are a variety of definitions of governance in general and IT governance in particular. Some regard governance as the means for enforcing external requirements on organizations, while others treat IT governance as the means for achieving the sort of benefits described above. There is a third set of definitions that focus on governance itself as a process. These operational definitions commonly focus on assigning decision rights.\(^1\) Often the decision-rights concept is augmented with decision mechanisms.\(^2\) Organizations that use these kinds of definitions are typically focused on driving greater efficiency (e.g., Lean Manufacturing).

Of course, there are hybrid definitions that combine these concepts. And there are other definitions that focus on the political roots of governance.

While each of these kinds of definitions contains an important perspective on governance, none of them is sufficient. Hence, there is no consensus on a single, concise definition. In this paper we adopt and build on the operational perspective.

A final point regarding the difficulty in defining governance: The natural language use of the term "governance" can get in the way. Sometimes we say we govern organizations, other times processes. Sometimes we explicitly say governance is carried out by governors who set policy and assign decision rights; other times we say decisions are governed by regulations or some external process. At times we focus on governance as a way of controlling individual and team behavior. In what follows, we discuss these perspectives on governance while focusing on what it takes to make governance operational. To ground this discussion, we propose an operational definition of governance, along with some supporting key definitions. These definitions, based on field experience, not only provide clarity for discussing governance, but also provide input to models and scenarios that can drive the design of technical and service assets.

To begin, we need a definition of "process":

A process is a series of actions, changes, or functions that brings about an end or result.\(^3\)

Processes are characterized by the changes of status of the artifacts/work products (objects) that occur as the processes are executed. It is also critical to note that processes may be hierarchical or related in some other way. For example, the overall development process involves the lifecycle of the overall product. It contains a quality or release management process that tracks the test coverage and test defect metrics, which in turn contains a defect management process that involves the lifecycle of a defect.

Now we can proceed with our operational definition of "governance":

*Governance is the process of:*
  * Establishing chains of responsibility, authority, and communication (decision rights)*
• Establishing measurement, policy, standards, and control mechanisms to enable people to carry out their roles and responsibilities

Note that this definition describes governance as a process. The objects under its control are the decision rights and measurements, policies, and control mechanisms. Every organization must establish the governance elements as specified in the definition that enable its business units to fulfill their role in and provide value to the broader enterprise. This specification is called the governance solution. As discussed below, this governance solution is established and maintained through the governance lifecycle and supported by aligned management solutions.

The first component of the definition for governance is common decision rights. This may be thought of as establishing the static side of governance, how the organization is structured and works. Specifying the decision rights puts in place the social network, allowing the members of the organization a clear understanding of who can be expected to make decisions. Some examples of decision rights include spending and hiring authority. For IT organizations, decision rights may include project funding, project content management, architecture content, and quality management. Note that we do not include project prioritization; this is an example of a decision that may be held by a line of business or higher cross-organizational authority.

The second component establishes the dynamic side of governance. Through instituting policies, standard measures, and controls, it is possible to establish governance decisions that can be enforced within the processes of an organization. Note also the emphasis on measurement; feedback loops are critical in any operation that requires improvement, and/or is subject to a changing environment.

Decision rights and metrics can be specified by considering what processes should be put under governance; decisions are made in the course of executing processes. In fact, as discuss below, choosing those processes to consider for applying governance is useful in that it can demonstrate to the business what is working and what is not, and how those processes may be changed to create greater benefit to the business. Briefly, we say the governance process is applied to the governed processes.

The governance solution

If governance is a process, the outcome of executing that process must be a set of tangible assets (sometimes called artifacts). We call the set of governance artifacts, the governance solution. A typical governance solution consists of some of the following:

• **Responsible Accountable Consulted Informed (RACI)** matrices for capturing the chain of decision rights and authorities.
• **Governance effectiveness measures** that capture at a business level how well the governed organization is delivering value to the broader enterprise, such as the average cost of a transaction. For the development function, an effectiveness measure could be time to delivery.
• **Operation metrics specifications** defining the day-to-day measurements as a basis for exerting control on the business processes. An example might be daily average response.
time. For the development organization, code churn -- the frequency of changes in program source code -- would be an operational measure.

- **Policy** libraries that document the guidelines and controls on the authorized decisions.
- **Compliance specifications** specifying which decisions must be documented to support audibility of the decisions.

**Governance and management**

Since managers make decisions, it is easily believed that management and governance are the same. However, management and governance take different perspectives. Governance generally looks at an organization from the outside, treating the organization as a system that needs to have the right structure and modes of operations to provide value. Management is inside the organization, ensuring those structures and modes of operations are executed.

Governance is about deciding the "who, what, when, why, and how" of decision-making. In particular, governing an organization includes:

- The decisions required by the organization (the "what")
- The roles (the "who") in the organization that are accountable for which decisions
- Policies that guide how the decisions should be made (the "why")
- The measures that enable informed decision-making (the "how")
- At what point in the governance process is the decision appropriately made? (the "when")

By contrast, management is the activity that ensures that the chosen governance approach is carried out day-to-day. Generally managers:

- Assign and supervise staff to roles
- Monitor the operational measures and execute the controls specified in the governance solution
- Collect and report on the governance effectiveness
- Do budget and resource planning and monitoring

**The governance lifecycle**

The governance lifecycle has four phases, as shown in Figure 2.

1. **Plan**
   - Capture the governance requirements needs of the organization such as meeting compliance needs, policy adherence, providing better business values, or meeting service levels
   - Determine financial and organizational responsibility for execution and testing of the solution based on the business requirements
   - Determine those processes to bring under governance
   - Determine the measures and targets of effectiveness of the governance solutions

2. **Implement**
   - Specify the decision rights, measures, and policies to be applied to those processes under governance
   - Specify the automation and tool support
• Roll out the governance solution to the organization in stages
• Monitor and measure
• Determine if the governance solution is meeting its effectiveness targets and make adjustments

3. Manage
• Have the organization execute governance solution to get a baseline of experience

4. Assess
• Collect governance effective measures
• Determine if the governance solution is meeting its effectiveness targets and make adjustments
• Analyze shortfalls to provide input to the plan phase of the next round of the lifecycle

Figure 2: The governance lifecycle

Governance considerations

As a process, operational governance must be carried out by one or more people. Even though it is useful to treat governance as outside the day-to-day operations (management) of an organization, those carrying out the governance process may or may not belong to the governed organization. Even so, those who are carrying out the governance process must be concerned with certain external forces on the organizations, illustrated in Figure 3, such as:

• **Processes carried out by the larger organization.** For example, most software development organizations are part of a business that executes a funding process larger than the concerns of the development organization itself. The broader organization commits funds, and the development organization commits to delivering something with given content on a certain schedule.
• **External policies.** Examples include corporate policies that affect the governed organization (e.g., mandates concerning equal employment opportunity affect the human resources organization) or organizational decisions to comply with external standards.
• **External standards.** Such as the various ISO specifications or less formal standards such as CobiT, ITIL, or Capability Maturity Model Integration (CMMI).
• **Government regulations.** Including Sarbanes-Oxley, or various industry specific regulations.

Figure 3: Forces affecting the governed process

In each instance, we say informally that the organization’s processes are governed by these external processes, policies, or standards. More formally, we mean that those executing the governance process must consider these forces in designing the governance solution, and those managers and staff executing the governance solution must be cognizant of these forces.

An important instance of this nested governance stems from the fact that organizations are contained within other organizations. For example, departments are contained in businesses, and the containing organization may have processes or policies that require certain decisions to be made regarding the contained organization. As such it is a governing process; it imposes constraints on those executing the formal governance on the contained organization. Conflicting policies may result without higher level operational governance. For example, the IBM® Rational® software group brand is contained in the IBM Software Group (SWG). There is an SWG process called "Integrated Product Development (IPD)" that the group brands (Rational, Tivoli®, etc.) use to set priorities and manage investments. Hence we say "IPD governs Rational processes." To execute IPD, certain artifacts must be generated. These artifacts have a lifecycle with decision points and thus require governance. This example of development governance provides individual brands with management flexibility while ensuring consistent investment decision-marking.

The contained organizations will have processes that enable it to participate in the governing process and, perhaps, do other things. These processes may not be explicitly required by the governing processes. These internal processes will need a good governance solution to improve the overall performance of the contained organization.

To net this out, the governing process imposes constraints on the governance solution of the contained organization. Note that this definition is consistent with much of the literature on governance, and it covers the application of governance to a family of processes as well as to the organizations carrying out those processes.
Value to the business

As pointed out by Michael Treacy and Fred Wiersema, there are three ways that a business may provide value in the marketplace:

- **Product innovation**: consistently delivering new products or features early to the marketplace
- **Operational efficiency**: consistently delivering commodity products or services reliably at low cost
- **Client intimacy**: rapidly responding to customers' evolving needs

Treacy and Wiersema point out that every company must provide some mix, but one of these three should dominate the culture and business value measures, as illustrated in Figure 4 (where the sample business appears to be dominated more by operational efficiency than by client intimacy). Because IT is key to providing this value delivery, it is important to understand that a mix of value propositions complicates IT governance. Some IT projects support one value, say delivering efficiency, while others may provide innovation. The governance effectiveness measures for the organization as a whole should reflect the mix while the governance solutions for the different projects are different. This mix should be considered during the plan phase of the IT governance lifecycle.

![Figure 4: The business value space](image)

Risk management

Risk is an identified uncertainty of the governed organization delivering value and meeting stakeholder needs. Commonly, there are three kinds of risk adopted that should be addressed by IT governance solutions:

- **Operational**: Risk assumed in the course of doing day-to-day business
- **Investment**: Risk assumed in developing or acquiring new capabilities
- **Legal**: Risk of being fined or sued, or going to prison for failing to meet legal requirements

When creating the governance solution, one must not only identify the organization goals, but also the risks mitigated by the IT systems. Generally, dealing with these risks is addressed by explicit processes: Operational risks might be addressed through security management, business
resilience management, and data integrity management processes. Investment risk is addressed through development, delivery, and integration processes. Therefore, the governance solution should place these processes under governance. The governance effectiveness measures should reflect the mitigation of these risks.

Legal risk is addressed by the compliance practice described below.

**Compliance**

Compliance is the documentation of the proper execution of decisions. Many organizations are introduced to governance concepts as they begin the process of complying with business regulations such as Sarbanes-Oxley or Basel II. These regulations are enforced by audits that determine whether or not business decisions were made by the appropriate staff according to appropriate policies. To pass these audits, organizations must document their decision rights, policies, and compliance records documenting that each of the decisions was in fact made by the appropriate person according to policy.

In establishing governance, an organization must consider its regulatory compliance needs and put in place procedures and tooling to efficiently capture compliance records, thus enabling an organization to record and communicate the extent to which various processes are executing in compliance with business or regulatory policies.

**Policies**

A policy is a rule or principle that guides or constrains the behavior someone given decision rights. Policies guide decision rights, which are generally conditional. For example, a first line manager might be allowed to spend money without further approvals below a set figure, and for expenditures above that amount, further approvals may be required. A hiring manager may fill a vacancy but cannot hire a relative. Policies provide guidelines for decisions, set the rigidity for following the guidelines, and may provide for exceptions. For example, federal judges are granted decision rights for sentencing those convicted of a crime, but they are often constrained by sentencing guidelines.

Policies may refer to the governance measures. For example, in an IT organization, a policy may require that the operations manager establish mitigating actions when certain quality-of-service levels are not met.

Note that policies not only constrain decisions, but may also require decisions to be made. For example, a manager may be required to establish and enforce equal employment opportunity practices.

Policy provides guidelines, sometimes sets limits, and sometimes enables behavior. This is similar to the notion that in certain political systems, citizens have every right except those explicitly prohibited by the state (i.e., these policies set limits). In other systems, citizens have only those rights permitted by the state (i.e., these policies enable behavior).
Principles of operational governance

Here we describe seven principles for operationalizing governance:

- The Process Principle: Governance is a process that is itself applied to processes to be governed.
- The Artifact Lifecycle Principle: The governed process artifact lifecycles guide the governance solution.
- The Risk Principle: Measures and controls must be adjusted according to the level of risk.
- The Suitability Principle: The needs of the organization determine how the level and style of governance will be tailored.
- The Behavior Principle: The governance solution drives the organizational behavior.
- The Deployment Principle: The governance solution must be implemented incrementally.
- The Automation Principle: Technology makes the governance solution empowering and unobtrusive.

The Process Principle

The Process Principle states, "Governance is a process that is itself applied to processes to be governed."

It is important to clarify how governance is applied to an organization. It is easy to get confused when one thinks about all the different concepts related to governance. It is an important analytical simplification to understand that:

- We apply policy to processes.
- We apply standards to processes.
- We enforce decision rights in processes.
- We measure and control processes.

It follows that to do governance well, governance must be a process with a sequence of operations (a lifecycle) and a set of objects (artifacts) that are created and evolved through its execution. The governance lifecycle is depicted above in Figure 2: The governance lifecycle.

Examples of governance artifacts are

- The RACI matrix tracks for a given decision who are
  - Responsible (those who do work to achieve the task, there can be multiple resources responsible both functional and financial)
  - Accountable (the resource ultimately accountable for the decision)
  - Consulted (those whose opinions are sought for validation)
  - Informed (those that are kept up-to-date on the decisions providing oversight)
- Repository authorization specifications
- Measurements specifications and templates
- Compliance records
These artifacts and possibly others are created and evolved throughout the execution of the governance lifecycle. The governance solution is defined as the overall set of governance artifacts and their dependencies.

Note that in this lifecycle, governance objectives are set and measures are defined to determine if the objectives are being met. It is a cyclical lifecycle that enables and requires that the governance solution be revisited periodically to see if the objectives are being met and to adjust the governance solution.

In carrying out the governance process, in the initial phase, one must determine the governed processes -- i.e., those organizational processes to which decision rights and measures are assigned.

A source for process specifications might include:

- The IT capability frameworks such as CobiT and ITIL, which define a set of processes executed by an IT organization
- Development maturity models such as CMMI, which define processes that are executed by software and systems development organizations
- The IBM SOA Foundation, which lists SOA-specific processes in the SOA lifecycle (model, assemble, deploy, manage)
- Any of a myriad of other domain-specific and business processes

It is useful, in fact, to define kinds of governance (IT governance, development governance, etc.) by specifying which processes are brought under governance. For example, applying governance to IT processes is IT governance, etc.

Some processes such as service reuse are often termed "governance processes" because they are very difficult to achieve without effective governance or because they further some governance goal. Strictly speaking, however, such processes are not governance processes; they are processes being governed.

Many things called governance processes are actually processes that are affected by or required for the execution of the governance solution. For example, to meet corporate security needs, an IT organization is tasked with creating and implementing a password policy. This mandate requires that the IT organization put in place a set of processes to create, and maintain, monitor, and enforce passwords. In the course of doing this, the leadership of the IT organization adopts the set of decision rights (e.g., who is accountable for approving access, issuing passwords, and changing passwords), internal policies, control mechanisms, and documentation procedures. Establishing this response to the mandate is governance. On the other hand, the day-to-day execution of the password policies is not governance, but simply password management. This IT organization further decides to implement this governance solution using password management software that automates and enforces the decision rights. The implementation and configuration of this software is determined by the governance solution, although those executing the password policies and using the related software are not doing governance; those policies and the supporting technologies are essential to executing the governance the solution.
Distinguishing governance processes from processes being governed helps clarify roles, the model of the processes themselves, and the level of governance required. It also helps clarify discussions of how and where runtime and tools support can help in governance.

**Artifact Lifecycle Principle**

The Artifact Lifecycle Principle states, "The governed process artifact lifecycles guide the governance solution." This principle builds on aspects of two earlier concepts: (1) governance includes the assigning of decision rights and (2) governance is applied to governed processes. Recall from the definition that execution of a process entails creating or changing the process artifacts.

Governance may be characterized by the sorts of decisions that need to be made at certain control points within the process. Control points provide an opportunity to measure the process and decide whether the execution of the process needs adjusting. Some of these decisions may require a set of measurements to be collected by a monitoring tool at any control point within the process. Knowing what decisions within the process are critical, and when to make them, and understanding what measurements are needed as input to those decisions, are all part of governance.

Certain activities within a process may be associated with a control point. For example, a "review step" of an artifact may be associated with a control point. In a similar fashion, certain events such as lifecycle milestones within the process itself may also be control points. In the IBM® Rational Unified Process® (RUP®), there are four phases: Inception, Elaboration, Construction, and Transition. At the end of each phase there is a phase transition revision at which the program management decides if the program is ready to move to the next phase (the end of Transition is product release). Each of these milestones is a control point.

At its essence, the artifact lifecycle provides a way to identify control points and to reason about defining the governance solution:

- Identify the processes to which governance will be applied
- For those processes, identify those artifacts created or affected by the process
- For those artifacts, identify when they change status or state (these are control points)
- At each control point, identify
  - The RACI roles for the decision
  - The applicable policies
  - The measures that should be applied and collected
  - The compliance records to be generated

This straightforward approach creates the elements of the governance solution to be implemented and automated.

In applying this workflow there are some additional considerations:

- Some processes, such as software development, may contain a set of sub-processes. In this case, the overall process has decision points (such as lifecycle phase transitions) as well as
each of the sub-processes. The decision points for the overall and sub-processes may or may not align.

- Not all artifacts need to be brought into the governance solution. It is a governance decision to determine which artifacts require formal lifecycle process modeling and governance, and which ones will be subject to informal or "ad hoc" management.
- In process engineering, a process itself is an artifact and there are control points associated with its lifecycle from proposed to adopted to retired.
- It is also important to consider how "collections" of artifacts jointly transition their lifecycles in some coordinated fashion.

Although much tooling exists already for modeling lifecycles of single artifacts and enforcing policies and decision rights at various points within the lifecycle of a single artifact, there is further work to do in order to understand more complex processes that orchestrate multiple artifacts simultaneously, and therefore to understand which control points within those processes need decision rights applied, measurements taken, and policies enforced.

An analysis of the artifacts being manipulated and a model of the lifecycles of those artifacts provide a rich set of processes for governance consideration. Much of the existing governance tooling, particularly registry-based governance, involves a model of key artifact lifecycles and provides control points for policy and decision rights enforcement.

**The Risk Principle**

The Risk Principle states, "Measures and controls must be adjusted according to the level of risk."

The Behavior Principle (see below) states that some process risks are associated with statistical uncertainty in the execution variables. The level of risk drives how you measure:

- When levels of certainty and process predictability are high, you can focus on measuring activity.
- When the levels of certainty are low, you need to focus on measuring the change in the level of certainty, not the individual activities.

Note that when levels of certainty are low, you cannot create a start-to-finish plan. Instead, you have to create a series of iterations using the results achieved and insights gained to set the activities and resources to steer the program to success. The key to success is effective measurement of each iteration, and the use of that measurement as feedback to the next iteration.

Often we fail to distinguish between high- and low-certainty situations. Admitting that you are in a low-certainty situation may be painful, because risks and costs are higher. Many organizations waste a tremendous amount of time dealing with postponed decisions, which raises the cost of business significantly. By ignoring the lack of certainty, you may avoid some pain temporarily, but this doesn't change the nature of the project and it creates a greater pain later.

**The Suitability Principle**

The Suitability Principle states, "The needs of the organization determine how the level and style of governance will be tailored."
Different organizations have different governance needs. Some organizations deal with highly regulated processes that have mission-critical or life-critical products, such as avionics or pharmaceuticals. These organizations need more formal, auditable governance. Other organizations, such as open source communities, are governed as more meritocracies with emergent behavior.

The need for stricter governance is met with tighter policies at the decision points along with ongoing policy enforcement and compliance measurement.

Even within an organization, different processes may require different styles of governance. Some processes, such as code release, require stricter governance than other processes, such as software coding.

Some governance styles need to consider the relationship between an organization and its sub-organizations. Different organizational cultures require different levels of autonomy in decision-making. For example, the decision-making rights between line of business IT organizations and cross-line of business (i.e., corporate) IT organizations vary between different businesses.

In an effort to become more agile and efficient, many organizations are adopting governance methodologies. Many methodologies vendors have created are all-encompassing framework approaches to meet the widest possible set of needs. Heeding the suitability principle, an organization must take a critical look at these governance methodologies and tailor them appropriately. The goal is to create an approach that fits the organization without losing the value of the structure a given methodology brings.

**The Behavior Principle**

The Behavior Principle states, "The governance solution drives the organizational behavior."

Long ago, managers gave up the notion that workers can be treated as programmable machines. Today, an executive’s challenge is to create the environment that results in the organization performing in such a way that its objectives are met. Governance is a tool that can be used to drive organizational behavior.

The applicability of governance to driving behavior follows from these four phenomena:

1. People spontaneously create their own social webs to get their work done.
2. Communications across an organization's boundaries is less efficient than those within its boundaries.
3. Diseconomy of scale -- communications grow nonlinearly\(^8\) with the size of the extended organization.
4. People will respond to how they are measured and how their organization is measured.

By properly setting decision rights and measures, one can use these phenomena to achieve good organization behavior. Similarly, these phenomena can lead to poor organization behavior if decision rights and measures are set poorly or not at all.
The first three phenomena relate to decision rights. Setting clear decision rights gives the staff an understanding of where their responsibilities lie and who needs to discuss what with whom. Further, a time-tested way to deal with phenomena 2 and 3 in development is to align organizations boundaries with system architecture. It is sometimes said, "You ship the organization." Logical decomposition methods work in business and enterprise architectures to encourage efficient communications. Setting authorities and decision rights reinforce these management techniques.

Experience has also shown that measures need to be chosen carefully as they may have great impact on the behavior of the system. Indeed, a management maxim is, "You get what you measure." For example, if you measure lines of code per software developer, the team will generate programs with lots of unnecessary lines of code.

The Deployment Principle

The Deployment Principle states, "The governance solution must be implemented incrementally."

Governance, because it is idiosyncratic to an organization, requires an incremental approach for an organization to adjust and get tuned. This principle emphasizes the iterative approach to defining and refining the governance processes and capabilities used within an organization. Governance capabilities include formalizing processes and best practices associated with the various governance disciplines, and establishing cross-discipline capabilities and services to make governance processes more efficient and cost-effective.

IBM recommends that organizations use the governance lifecycle to incrementally identify governance needs, put governance capabilities in place, and establish measurement mechanisms to ensure that the improvements to governance cause the desired change in the behavior of the organization.

There are three reasons to iterate in the governance lifecycle:

- To incrementally add new governance capabilities
- To incrementally improve on existing governance capabilities
- To incrementally transform organizational capabilities responsible for governance

If you tackle too big a problem in your first attempt to upgrade your capabilities, you increase the probability of failure. Don't bite off the entire governance problem all at once; prioritize your governance needs during the planning phase and count on traversing many times the steps described in the "Governance Lifecycle" section of this article. Getting governance right is an iterative process; the cultural and behavioral aspects of governance make it a non-deterministic activity.

An organization's propensity toward "governability" will be a major factor in its ability to adopt a governance strategy. Those companies with a heritage of structure and accountability will be more adaptable to governance, and those companies that have taken the "cowboy way" will struggle more. Some examples of this principle are the longevity of companies like IBM and GE. Each of
these companies has a long history of structured governance, which has given them the ability to weather difficult times.

**The Automation Principle**

The Automation Principle states, "Technology makes the governance solution empowering and unobtrusive."

Since governance generally comes from outside the organization or is seen to meet external needs, the workers may perceive governance as a necessary evil, and the new requirements can indeed add overhead and impede productivity. Technology can address this concern by automating the choreography of decisions, capturing compliance records, collecting and integrating the measures, and, perhaps, by enforcing policies that make the governance solution part of the organization's fabric.

A good governance solution can empower an organization. Well-specified decision rights provide clarity of roles and facilitate communications. Everyone has a clear idea of what communications need to occur to complete a task. Good measures reinforce the right behavior. Reinforcing the governance decision with automation provides a means for reducing overhead and ensuring the continued execution of the governance solution, raising staff's confidence that the solution is real and will be followed. In the end, the governance solution should fade into the background, allowing the workers to focus on their real work.

**A final thought**

People often think they have a choice between "governance" and "no governance," but in reality the choice is between "good governance" and "bad governance." Every organization has a framework of decision-making and some set of often unstated measures. The needs of the business and the role of IT evolve; these unintentional governance solutions do not. Good governance is intentional, and it takes effort and attention. The operational perspective described in this article provides an approach for doing governance well.

**Notes**


2. According to the IT Service Management Forum (itSMF). For more information, see [http://www.itSMF.org/](http://www.itSMF.org/)


7 If you're unfamiliar with the RACI diagram, Wikipedia offers a good overview at http://en.wikipedia.org/wiki/RACI_diagram


© Copyright IBM Corporation 2007
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)