

# IT Governance Defined

---

IT Governance allows senior management the ability to manage the enterprises IT resources; to direct, evaluate and control its use and implementation to achieve the strategic goals of the organization. IT resources are leveraged by leadership, organizational structure and processes to produce required information and drive the alignment, delivery of value, risk management, optimal use of resources and performance management.

## Risk Assessment Methodology Overview

The three (3) sides of the IT Governance triangle are people, process and technology. These three principals together provide the management system to oversee the resources and the activities taken to produce the information that supports the organization's strategic goals.

Many different approaches to risk assessment have been developed. RGW Associates has taken the best of these and distilled them into 9 key components. The following guidelines provide a simple step-by-step explanation of this process.

### General Guidelines for a Risk Assessment

#### 1. Engage a world class risk assessment team

- ✓ RGW Associate's expert risk assessment team is responsible for the collection, analysis, and reporting of the assessment results to your management. RGW Associates will insure that all aspects of the activity work flow are represented on the team, including human resources, administrative processes, automated systems, and physical security.

#### 2. Set the scope of the project

- ✓ The RGW assessment team will identify at the outset of the engagement, the objective of the assessment project, department, or functional area to be assessed, the responsibilities of the members of the team, the personnel to be interviewed, the standards to be used, documentation to be reviewed, and operations to be observed.

#### 3. The RGW team will identify assets covered by the assessment

- ✓ Assets may include, but are not limited to, personnel, hardware, software, data (including classification of sensitivity and criticality), facilities, and current controls that safeguard those assets. RGW Associates will identify all assets associated within the scope of the assessment project.

#### 4. Categorize potential losses

- ✓ RGW Associates will help in the identification of the losses that could result from various types of damage to an asset. Losses result from physical damage, denial of service, modification, unauthorized access, or disclosure. Losses may be intangible, such as the loss of the organizations' credibility.

#### 5. Identify threats and vulnerabilities

- ✓ A threat is an event, process, activity, or action that exploits a vulnerability to attack an asset. RGW Associates expert team will identify all the potential threats and vulnerabilities including but not limited to natural threats, accidental threats, human accidental threats, and human malicious threats. These could include power failure, acts of nature, or hardware/software failure, data destruction or loss of integrity, sabotage, or theft or vandalism. Vulnerability is a weakness which a threat will exploit to attack the assets. RGW Associates will identify vulnerabilities by addressing the following while the RGW team performs its initial data collection process:

- physical security
- environment system security
- communications security
- personnel security
- plans
- policies
- procedures
- management

**6. Identify existing controls**

- ✓ Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. The experts at RGW Associates will identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.

**7. Analyze the data**

- ✓ In this phase, all the collected information will be used to determine the actual risks to the assets under consideration. A technique to analyze data includes preparing a list of assets and showing corresponding threats, type of loss, and vulnerability. Analysis of this data should include an assessment of the possible frequency of the potential loss.

**8. Determine cost-effective safeguards**

- ✓ RGW Associates Includes in its assessment, the implementation cost of the safeguard, the annual cost to operate the safeguard, and the life cycle of the safeguard.

**9. Report**

- ✓ The type of report to make depends on the audience to whom it is submitted. Typically, a simple report that is easy to read, and supported by detailed analysis, is more easily understood by individuals who may not be familiar with your organization. The report should include findings; a list of assets, threats, and vulnerabilities; a risk determination, recommended safeguards, and a cost benefit analysis.

## How to measure capabilities

Organizational capabilities can be measured using a maturity model (such as the one provided by the CobIT Management Guidelines) to track the ability of that organization to consistently deliver the expected outcome. There are five levels defined in the Capacity Maturity Model (CMM), it has been shown that the effectiveness, and control of an organization's software processes are improved as the organization moves up these five levels. The five levels are as follows:

Level 1 - Ad hoc (Chaotic)

It is characteristic of processes at this level that they are (typically) not documented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

2

Level 3 - Defined

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

#### Level 4 - Managed

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

#### Level 5 - Optimizing

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

At maturity level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, shifting the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.

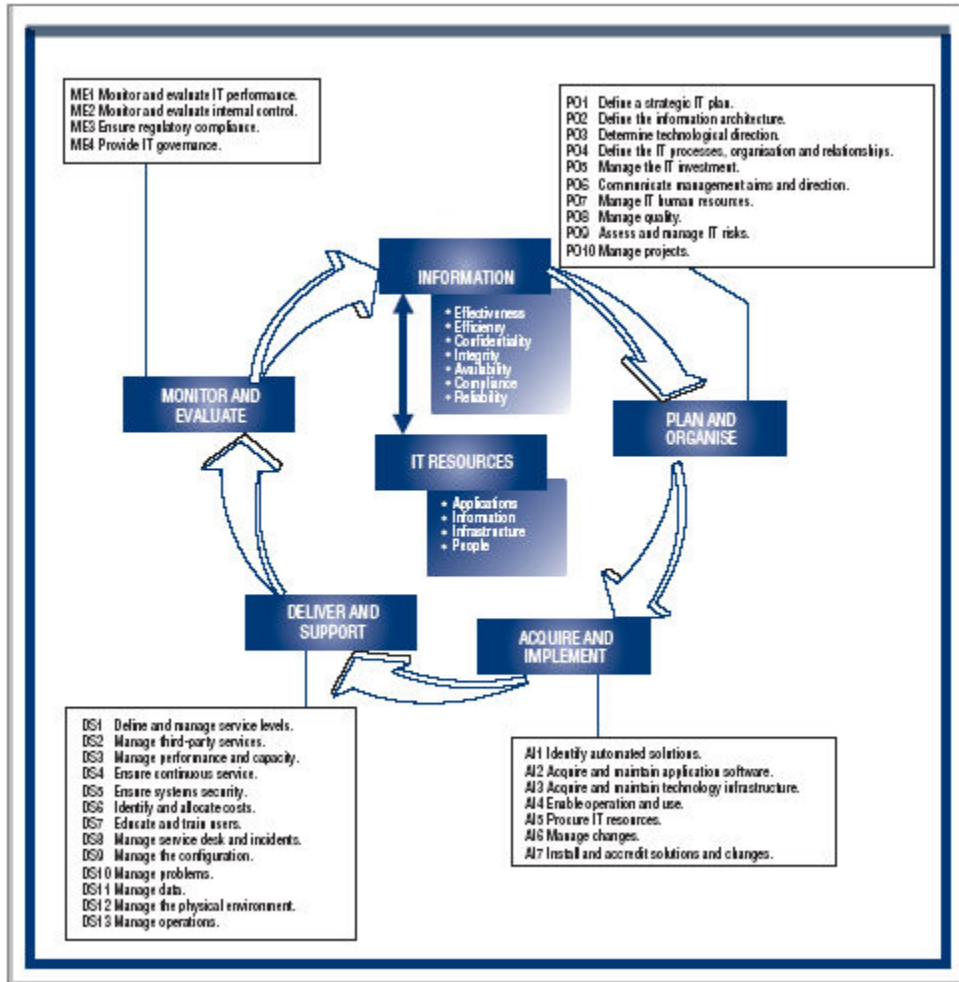
Within each of these maturity levels are Key Process Areas (KPAs) which characterize that level, and for each KPA there are five definitions identified:

- Goals
- Commitment
- Ability
- Measurement
- Verification

The KPAs are not necessarily unique to CMM, representing — as they do — the stages that organizations must go through on the way to becoming mature. Process assessments are led by a skilled/competent lead. The organization's process maturity level is assessed, and then a specific plan is developed to get to the next level. Skipping levels is not allowed.

## CobIT and its place in the IT organization

*Control Objectives for Information Technology* (CobIT) is a comprehensive set of resources containing all the information that an organization requires to adopt an IT governance and control framework. CobIT provides best practices across the domain and process framework presented in a manageable and logical structure. CobIT is strongly focused on control and less on execution allowing greater latitude to the IT administrator regarding compliance to specific objectives; optimizing IT-enabled investments, ensure service delivery and a measure to judge against when things do go wrong.



## Understanding and Setting Stakeholder Expectations

Another challenge to implementing a solid IT Governance framework involves managing the stakeholders expectations when multiple agencies or departments own or use the same set of services and where applications are owned by individual units who control design, development and support budgets.

Successful adoption of a solid IT governance standard requires full support of senior management and must be conducted by teams that include both functional managers and information technology administrators. RGW Associates works closely with every level of management and technology administrators to insure full buy-in by all stakeholders.

## Accountability plays an important role

Establishing accountability is the first and most important step towards better governance. This is achieved by examining the roles and responsibilities within the decision making processes. Only when accountability is fully established can any governance directive be successful.

## What role does process play

Processes are defined to organize activities efficiently and effectively. Processes exist throughout the enterprise and are all influenced by organizational structure and leadership. Implementation of IT Governance requires repetitive steps and occurs at the tactical, strategic and operational levels in line with stakeholder priorities.

Developing a governance framework involves people, processes and technology and requires establishing measurable preconditions that can be met while managing outcome to be consistent with those reconditions.

The purpose is to establish discipline and maturity in IT processes as an accepted part of the organization thereby gaining greater control and economies while achieving the organization's strategic goals.

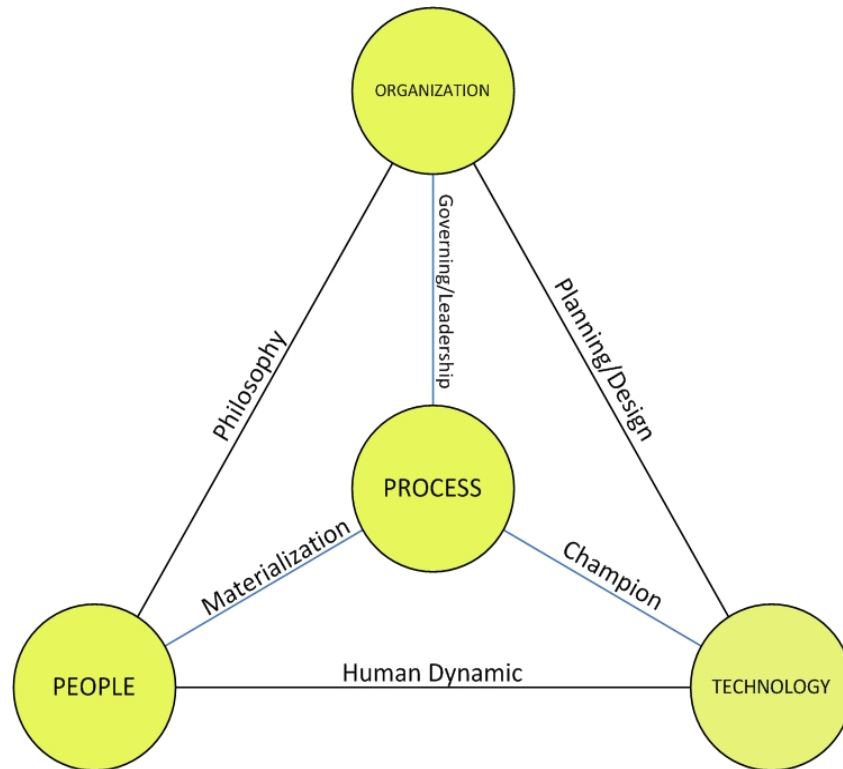
IT Governance has become an integral part of corporate governance consisting of three (3) main precepts:



Organization

Technology

People



These fundamental components are all brought together by **process**. Process is the most enduring of all components of a management system.

Process ensures stable, controlled services which are repetitive while also being measured objectively against deliverables and a predefined set of metrics.

The dangers of blurred organizational boundaries that have become more prevalent with the onset of e-commerce and decentralization must be kept in mind by directors and executives; these happenings result in governance responsibilities that now go well beyond the traditional boundaries. Care must be given that IT Governance is integrated throughout the entire value chain.

## Components of a Risk Assessment

RGW Associates LLC categorizes a risk assessment into three (3) major components. RGW Associates classifies these as follows:

### 6 Administrative Safeguards

These include, but are not limited to, those control measures that ensure:

- o classification of data handled by the unit and determination of controls to protect those assets;

- documentation of procedures, standards, and recommended practices to ensure that applicable policies and controls are implemented appropriately for a given business process;
- identification of personnel who are authorized to access systems;
- assurance that appropriate authorization controls are implemented;
- security awareness training and education for all personnel; and
- background checks prior to the selection and hiring of new personnel into critical positions.

### Logical Safeguards

These encompass the range of technical controls that:

- ensure access by only authorized users and session termination when finished;
- enforce secure password management;
- manage tracking of development, maintenance, and changes to application software and information systems;
- manage access to the network
- ensure event logging

### Physical Safeguards

These protect physical resources through controls that:

- allow access by only authorized individuals, through the use of physical means, such as locks, badge readers, or access cards;
- ensure the prevention, detection, early warning of and recovery from emergency disruptions, such as flooding, power failures, or earthquakes
- govern the receipt and removal of hardware and electronic media, including equipment reassignment, and final disposition of equipment

## Getting Started

A solid process framework is essential and should be the centerpiece of any IT improvement initiative. This framework should reflect the common understanding of how procedures and activities are grouped and what outcomes are expected. Regardless of the improvement effort, whether it is risk management, technology assessment or workflow improvement, a strong process framework will make the scope of each process and the expected result easier to communicate.

Numerous related activities and interfaces make up a process that together result in the achievement of the predefined result. While it is possible to create your own process framework, it will require great effort both in development and acceptance by the stakeholders. It is therefore far better and easier to begin with a well defined framework that is widely accepted as “best practice” by the broader user community.

## **The role RGW Associates plays**

RGW Associates LLC is a recognized name in providing organizations and government agencies comprehensive compliance and IT governance solutions. Through the use of our “Best Fit” purpose-built process, RGW Associates is able to deliver a high value, customized framework that fits the requirements of our customer. Following strict guidelines set forth by industry recognized Risk and Governance standards, RGW Associates implements solutions according to the National Institute of Standards and Technology (NIST), (specifically Special Publication (SP) 800-30, SP 800-27 and SP 800-14) as well as CobIT (CobIT 4.1) and other directives issued by the IT Governance Institute. RGW Associates is an active member of ISACA and therefore is bound by all principals, standards and guidelines and the Code of Ethics set forth by that organization.

