GOVERNANCE AND IT MANAGEMENT IN 30 AUDITS

In the Public Administration, governing information technology (IT) has one goal: to deliver results to organizations, citizens and society.

Also known as "value creation", the expression "results delivery", in IT, according to good practices, amounts to performing three activities well: guaranteeing the delivery of benefits, optimizing the use of available resources and maintaining risks at acceptable levels. In seeking to understand and assess how the Federal Public Administration (Administração Pública Federal - FPA) has organized itself in IT to perform these three activities, there were 30 audits carried out, between April of 2013 and September of 2014.

Since 2007, Sefti has been collecting information on the state of IT governance together with the organizations that comprise the APF. During this period, there have already been four surveys: 2007, 2010, 2012 and 2014. After each survey, there is a series of audits in order to ascertain, in a subset of federal public organizations, whether the situation reported by the managers corresponds to reality, as well as collect the best practices and assist in their dissemination to other organizations.

Goal of external control

After the third edition of the survey, in 2013, Sefti realized that it was necessary to advance in the assessment of the mechanisms of IT governance and management, with the goal of attributing greater weight to the analysis of results effectively delivered and how the risks have been mitigated. In this context, the present study came about.

The audit was divided into two phases. The first involved 24 audits with the goal of assessing the implementation of controls informed in responses to the TCU surveys, as well as analyzing the responses presented. The second involved six audits, five of them carried out in organizations that have high IT governance rating, according to the surveys conducted by the TCU. The greater complexity of the controls assessed in the second phase was the main difference between the two stages. The purpose was to gather experiences and good practices of organizations that were more mature in terms of governance and IT management, and, at the same time, assess the causes of the problems and difficulties reported by first group of organizations.

Main findings of the TCU

In the first phase, the reports indicated problems and difficulties in all the organizations audited. While advances were perceived in some organizations, in others the responses presented in the questionnaire did not correspond to reality: in one body, inconsistencies were found in 30% of the responses presented to the TCU. In general, they are examples of areas, which continue to represent challenges: the acting of high administration in the governance of IT issues; service-level management; and information security.

In the second phase, the negative points were few in number, while good practices resounded. Good examples, such as the effective monitoring of IT projects and goals, practiced in the Central Bank of Brazil and the Hydroelectric Company of San Francisco (Chesf), were identified and reported. The adoption of good practices and controls, alone, does not ensure project success; yet, it very much favors obtaining positive results.

Topic	Main findings in the audits of the 1st phase
Questionnaire	The answers provided by the organizations during the PerfilGovTI TCU Survey, of 2012 had reasonable reliability (average inconsistencies per organization of 8.71%).
Governance	There is a distancing of high administration in relation to IT matters. The majority of the organizations do not have an organized process oriented toward the improvement of IT governance.
Strategy and Planning	46% of the organizations audited in the Executive Branch have neither IT Strategic Planning nor even a formalized and published IT Director Plan. Advances were identified in the Judiciary Branch and are attributed to greater regulation of this practice in this Branch.
Information Security	Inadequate planning and absence of consistent risk analyses that support information security actions. Recurrent failures in the establishment of processes such as: business continuity management, access control, information security risk management and incident management.

Topic	Main findings in the audits of the 2nd phase
Strategy and Planning	Mature practices for monitoring the goals and targets formulated in the IT plans and for the selection and prioritization of projects were identified.
IT Results	Applied research revealed perception that the systems effectively contribute to the achievement of organizational results; high degree of satisfaction with the basic computational structure (workstations, electronic mail, internet, and printers); high dissatisfaction rate with time taken to meet systems requirements (maintenance, changes, and corrections).
Risk Management	The practical actions of IT risk management, many times are performed exclusively by IT, remaining separate from corporate risk management.
Resource Management	Indirect IT costs, like the costs with human resources, are not duly assessed and incorporated into the overall cost of IT actions.

The TCU's Deliberations

In addition to specific referrals addressed to each audited organization, the final report contains the determinations and recommendations to Superior Governing Bodies (Órgãos Governantes Superiores - OGS). Among them, the Department of Coordination and Governance of State-Owned Enterprises (Departamento de Coordenação e Governança das Empresas Estatais) and the Secretariat of Logistics and Information Technology (Secretaria de Logística e Tecnologia da Informação), both linked to the Ministry of Planning (Ministério do Planejamento), as well as the National Councils of Justice (Conselhos Nacionais de Justiça) of the Public Ministry (Ministério Público). The OGS received recommendations designed to foster the improvement of performance and, consequently, the organizations under their supervision.

It was suggested that interlocution be improved between the OGS, to propitiate better use of the experiences and products developed by each of them, such as: guides, regulations and processes. Still recommended was the improvement of the overall driving strategy of information technology in the Executive and Judicial Branches. Also recommended was the adoption of sector-specific strategic planning for the information security of these branches, a way to provide systemic treatment for this issue, which still inspires care.

Expected benefits

The benefits expected from TCU's performance translate into the promotion of improvements in internal organization (governance, IT management) of the units audited, as well as of improved IT governance of all APF through guidance to the superior governing bodies.

Judgment

Judgment 3.051/2014-TCU-Plenary

Date of session: 5/11/2014

Rapporteur: Substitute Minister Weder de Oliveira

TC 023.050/2013-6

Technical Unit responsible: Department of External Control of Information Technology (Secretaria de Fiscalização de Tecnologia da Informação - Sefti)