Before 1999, the regulation and supervision of the banking system in Turkey had a fragmented structure in which the Undersecretariat of Treasury and the Central Bank of the Republic of Turkey were the main actors. Crises in the banking sector taught the necessity of effectiveness of regulation, supervision and the importance of independent decision-making mechanisms. By June 1999, the Banking Regulation and Supervision Agency (BRSA) was established according to the Banks Act Nr. 4389 and it began to operate in August 2000.

Similarly, the IT audit unit of BRSA is a byproduct of a massive IT-based financial fraud at Imar Bank. Responsibilities of this unit are onsite audit; authorization and enforcement activities regarding external audit institutions (EAI); enforcement activities regarding IT functions of banks; follow-up findings in the audit reports on information technology and business processes (ARITBP) prepared by EAI; drafting of legislation regarding the management, governance and audit of IT.

As the policy maker of the banking sector in Turkey, BRSA is responsible for designing the most suitable legislative environment for IT governance in banking. Therefore, BRSA has to keep up with new developments in IT governance frameworks. Since governance has been changed drastically with the release of COBIT® 5, compared to previous versions, a review of domestic banking legislation is needed. There are numerous similarities between the BRSA-created banking regulations in Turkey and the processes of the COBIT 5 governance area, including the adoption of many improvements over COBIT® 4.1. The BRSA IT audit concept consists of domestic regulations and incorporates the "current version of COBIT." Domestic regulations (figure 1) about governance of enterprise IT (GEIT), risk optimization, resource optimization, transparency, benefits delivery and additional legislation designed specifically for Turkey are described here. The results of this study are expected to be beneficial for decision makers in government bodies, banking industry, independent auditors and related stakeholders.

**GEIT: STRUCTURE, OPERATING INTERNAL SYSTEMS**

“Communiqué on the Principles to Be Considered in Information Systems Governance and Management in Banks (CPISGMB),” issued by BRSA, clearly states that GEIT is a part of corporate governance and the strategy of IT must be aligned with the bank’s strategies and objectives to carry out its operations in a stable, competitive and improving line. The structure of IT to be established within the bank must be commensurate with the scale of the bank and with the nature and complexity of the offered products and services. In addition, the first principle of the Corporate Governance Regulation of Banks (CGRB) states that corporate values and strategic goals shall be established within the bank taking GEIT principles into account.

To operate banks’ GEIT effectively and achieve their mission, BRSA has regulated the organizational structure—internal systems. Establishment of internal systems is intended to ensure the monitoring and controlling of risk to which banks are exposed, in all channels and partnerships subjected to consolidation. Internal systems consist of internal audit, internal control and risk management, and those units are established under the board of directors (BoD) within the institutional structure of the bank. For instance, the purpose of the internal audit system is to provide assurance to senior management (SM) that the activities of the bank are conducted in accordance with the law and other applicable legislation, the internal strategies, policies, principles, and targets of the bank and that the internal control and risk management systems are...
effective and adequate and provide communication of GEIT principles to top-level management (TLM).

The internal audit identifies any deficiencies, errors and abuses; prevents them from occurring again; secures the effective and efficient use of bank resources for resource optimization; and ensures the accuracy and reliability of information and reports communicated to the BRSA, SM and the public. The IT auditors are also included in the internal audit team and must have a minimum level of knowledge proven by education and certificates of related training areas. Also, a sufficient number of internal audit staff must be employed to fulfill audit services without delay. Risk management, internal control and internal audit mechanisms ensure effectiveness and performance of GEIT.

**GEIT: EVALUATE, DIRECT, MONITOR**

BRSA’s regulation logic is evaluate first, then direct, and finally monitor and intervene. This logic is imbued in all legislation. The responsibilities and accountabilities of the BoD, audit committee, SM, TLM and others are regulated clearly.

The BoD of the bank has the power and responsibility to determine the strategies of a bank and responsibilities of units; establish the internal systems in accordance with the procedures and principles specified in the ISB; operate them in an effective, adequate and suitable manner; ensure proficiency of internal systems’ staff; have knowledge on all risk factors of the bank and methods of measuring risk; approve and supervise the risk policies concerning risk appetite, monitoring, management and reporting; approve the information security policy of the bank; and secure the information provided from the accounting and financial reporting system. Additionally, the audit committee (AC), consisting of elected BoD members, supervises the internal audit function; establishes the channels of direct communication for reporting of irregularities to audit units; evaluates proposals of TLM concerning the internal systems; ensures and monitors the independence and performance of internal and external auditors; informs the BoD regarding AC’s responsibilities; and evaluates the availability of the necessary methods, tools and implementation procedures.
for identifying, measuring, monitoring and controlling the risk carried by a bank. The bank’s SM carries out efficient surveillance to manage the risk derived from the usage of information systems (IS) and establishes mechanisms to periodically evaluate threats, review and monitor IS policies that include appropriate approval steps, and increase awareness relating to information security. As stated in the ISB, the duties and responsibilities of TLM are to coordinate and monitor the bank personnel employed in departments (ISB-8/1), make timely and reliable reporting to the BoD about risk, and review and approve risk areas of projects on usage of new IS elements that will have important impacts.

GEIT: EXTERNAL AUDIT

The EAI is another key player in the Turkish banking sector. Therefore, BRSA directly deals with all details (e.g., adequate resources, qualifications, titles of members in an audit team) and regulates IT external audit activities based on the “Regulation on Bank Information Systems and Banking Processes Audit to Be Performed by External Audit Institutions” (RIBPEA) to ensure that IT-related processes are overseen effectively, are analyzed, and identify the internal and external environmental factors and compliance with regulations. According to the RIBPEA, the BoD of a bank must sign the audit contract of banking processes and IS. The auditor determines the audit scope of processes, systems, operations and control mechanisms based on a risk-oriented manner and considering the materiality criteria. Also, the auditor provides sufficient audit evidence to provide assurance. ARITBP, prepared and digitally signed by the EAI, are sent to the IT audit department of BRSA. If the BRSA’s IT audit department considers the content of the audit to be inadequate or not created properly, the BRSA can intervene and enforce the EAI to improve the audit content.

The audit of banking processes is performed every year; the audit of IS processes is completed every two years, per COBIT. If necessary, BRSA can change the frequency or scope of the audits for one bank or more. While evaluating the findings, if a notable or important lack of control exists, the auditor would check the unit or function for compliance. The auditors also inform TLM in writing or orally on any subject they deem important during the bank IS and banking processes audits.

If BRSA identifies that there are significant issues affecting banking processes/systems, the bank’s assets, activities carried out in accordance with internal policies and regulations, general banking practices, reliability and integrity of accounting and financial reporting, and timely availability of information, the EAI can be removed from the list of competent audit institutions. All of these are regulated by the provisions of articles 12, 20, 22, 25, 32, 36 and 40 of the RIBPEA to ensure that IT-related processes are overseen effectively and transparently to confirm the compliance of legal, regulatory and governance requirements.

RISK MANAGEMENT

As already mentioned, risk management is the main part of internal systems that guides GEIT by clear responsibilities given to the BoD, AC and TLM. According to article 5/1 of CPISGMB, “the bank takes necessary measures in order to measure, monitor, control and report the risks derived from IT usage in banking activities.” Article 5/2 of CPISGMB continues, “As well as the risk derived from IT are considered within the scope of operational risk, due to the possibility that these risks may be a multiplier of other risks derived from banking activities, an integrated risk management approach shall be adopted for all banking activities.”

Operational risk determines the amount of regulatory capital that banks must allocate. Therefore, operational risk is the digitization of IT and is important for enterprise governance. Since IT is an essential part of banks, interruption of services or the occurrence of IT risk puts banks in a difficult situation. According to the risk profile, operational structure and corporate management culture of the bank, it is essential that the bank develop risk management processes and evaluate the risk derived from IT accordingly. Therefore, risk tolerance related to the use of IT is understood, communicated and managed by determining the level of IT-related risk: The ratio of using IT support services increased in banking activities; business continuity of the bank and safety of data recorded, transmitted and processed became fully dependent on IT; and IT errors are different from familiar frauds. Basic responsibilities of the risk management department are to determine the risk management policies and procedures on the basis of the risk management strategies; ensure regular and timely reporting about risk measurement and monitoring results to the BoD and SM or relevant internal systems officer; and ensure that the risk factors, including IT-related risk, are understood, sufficiently evaluated and communicated with regard to the bank’s risk tolerance. The bank must also implement mechanisms to provide early warning information concerning
unexpected events related to IS. Appropriate communication channels must be established from bank staff to management, internal control and internal audit to minimize risk, identify it early and communicate risk tolerance.\(^\text{16}\) To manage IT-related risk, business continuity tests, including tests of all channels in a bank and support service organizations, if needed, must be completed once a year. Test results are reported to TLM. Based on the results, plans can be changed, including metrics of risk governance and management processes, principles of escalation, and technical details.\(^\text{17}\)

### TRANSPARENCY

BRSA is concerned with the proper functioning of the banking sector and recognizes that a key element for this is transparency. According to principle seven of CGRB, transparency must be ensured in corporate governance. Transparency in financial audit reports is 100 percent, while IT audit reports are transparent only to key stakeholders because of the nature of IT. If, for example, the findings of an IT penetration test\(^\text{18}\) were to be published, the bank’s systems could be easily hacked. In the same way, penalties regarding domestic banking regulations charged by BRSA are not published because of reputational risk. In brief, the defined key stakeholders, e.g., EAs, can have all the information about IT costs, risk and benefits. Additionally, transparency is meaningful if it is understood correctly. Therefore, BRSA regulations require the auditor to give detailed information about criteria, status, links to specific articles of the regulation, business risk from the findings as far as required by audit objectives and opinions of the auditee outcome assessment in ARITBP.\(^\text{19}\)

### IT BENEFITS

Banks establish policies, procedures and processes relating to the governance and management of IS. These are reviewed and renewed regularly to ensure that they are in line with technological developments or changes in the area of related business, and to optimize value contribution to the business.\(^\text{20}\) They also supply optimal value, adequate budget and resources, which shall be allocated according to article 4/1 of CPISGMB.

The banking sector is directly dependent on IT for even basic banking activities and business continuity. However, IT investments in banks must be at acceptable costs and must secure optimal value. For instance, the IS must be enabled to identify deviations from annual budgets and targets.\(^\text{21}\)

### ADDITIONAL LEGISLATION

Rather than imposing COBIT as the single set of rules governing IT processes in the banking sector, BRSA utilizes COBIT as a complementary source.\(^\text{22}\) That is, although COBIT is a comprehensive framework, relevant additional country-specific or risk-dependent legislation has been included by BRSA to be implemented by banks. For instance, to ensure ATM security, camera systems have become compulsory for each ATM.\(^\text{23}\) Another example is that banking business processes are to be overseen every year for six years\(^\text{24}\) to ensure that their concept is in parallel with COBIT DSS06 Manage business controls.

The Regulation on Management Assertion\(^\text{25}\) ensures that the BoD evaluates the effectiveness, adequacy and compliance of internal controls on IS and banking processes.\(^\text{26}\) Another responsibility of the BoD is approving and signing action plans\(^\text{27}\) that are used to follow up on the findings in ARITBP. If the solution or end date of findings changes, the BoD must approve the plan again. With this, the BoD must understand risk and follow up on IT findings. Additionally, CPISGMB mandates that the relevant risk implied by each of the IT audit findings be mapped into business risk\(^\text{28}\) and by independent auditors, so that the inherent risk can be easily perceived by TLM, most of whom do not have technology backgrounds. BRSA organizes frequent meetings with relevant stakeholders to discuss topics related to banking IT fraud cases and legislations and take complaints and other comments into consideration in preparing regulations. With the help of these meetings, BRSA acts proactively, rather than offering decisions in a reactive manner after realization of an undesired outcome.

If required, relevant IT and banking processes audit findings can be shared with other public authorities such as the Capital Markets Board and the Central Bank of the Republic of Turkey. These authorities may be informed so that they act properly in case legislation requires them to take actions. BRSA aims to provide communication and reporting mechanisms for oversight and decision making with appropriate information for all stakeholders playing a role in the banking sector.

### CONCLUSION

BRSA is the responsible governmental organization for designing the most suitable legislative environment for
IT governance in the banking sector of Turkey. Thus, a comparison of the COBIT 5 governance area with domestic BRSA legislation was completed.

In general terms, BRSA regulations had been in force before COBIT 5 was issued, and the processes newly introduced by COBIT 5 are largely covered by BRSA regulations. The study results show that there are numerous similarities as well as certain differences between the two. The differences may be attributed to two reasons: First, unlike COBIT, the BRSA legislations have been specifically designed for the banking sector. Second, domestic requirements are being considered in the design of the legislative framework for the Turkish banking sector in a continuous manner.

ACKNOWLEDGEMENT
The authors would like to thank Ahmet Turkay Varli, head of the IT department at BRSA at the time of this writing, for his invaluable support.

ENDNOTES
1 The Turkish banking system is composed of 49 banks, three of which are public commercial banks and four of which are participation banks. Total assets are approximately US $820 billion. In total, there are about 11,691 branches in Turkey. There are 41 independent IT auditing organizations licensed by BRSA to perform audits in banks, but only six of these are licensed to perform IT audits.
3 Fort, J.; P. Hayward; “The Supervisory Implications of the Failure of Imar Bank,” Commission of Inquiry into the Supervisory Implications of the Failure of the Imar Bank
4 Authorization refers to licensing activities.
7 BRSA, Corporate Governance Regulation of Banks (CGRB), 1 November 2006, www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemler/1682kurumsalyonetimyonetmeligiis_lemishali.pdf
8 Op cit, ISB, article 5; Banking Law No. 5411, article 8; CGRB, principle 3
9 The general manager and assistant general managers of a bank, the managers of the units included within the scope of the internal systems, and those managers of the nonadvisory units who serve in positions equivalent or superior to the position of assistant general manager in terms of their powers and duties even if they are employed with other titles.
10 Op cit, ISB, article 6
11 Op cit, ISB, and CGRB principle 4
12 Op cit, ISB, 8/1 and 5/2/i
13 Op cit, ISB- 26/5 and 26/6; CPISGMB 6/3
14 Op cit, RIBPEA 7/5 defines key words. “Control” represents policies, procedures, practices and organizational structures, aiming adequate assurance related to the realization of business objectives, prevention/identifying/correcting of adverse events. Similarly, “control weakness” is the case of determining the state that design or operation of a control prevents errors.
15 Op cit, ISB 40
16 Op cit, ISB 12/3
17 Op cit, ISB 13/11
19 BRSA, “Communiqué on the Report Relating to Information Systems and Banking Processes Audit to Be Performed by External Audit Institutions (CIPBEA),” 13 January 2006
20 Op cit, CPISGMB 4/2
21 Op cit, ISB, article 11
22 Op cit, CPISGMB 22/2 and 34/1, RIBPEA 24/2
23 Op cit, CPISGMB 32/10
24 Op cit, CPISGMB 21
25 RSA, Circular on Management Assertion, 30 July 2010
26 RIBPEA 19/7 and 33
27 Op cit, RIBPEA 19/8
28 Op cit, CIBPEA 9