Using COBIT 5 to Assess IT Processes Capabilities and Evaluate Compliance With the World Lottery Association Security Control Standard and ISO 27001

By Ioannis Panopoulos, CISA, CRISC, CGEIT, CSXF, ISO 27001 LA, and Marisa Melliou, CISA, CAML, CCO, CIA, CRMA, CRP, ISO 27001 LA

COBIT Focus | 16 October 2017

The internal audit team of one of the biggest gaming operators in Europe implemented a cloud-based governance, risk and compliance (GRC) platform to improve the quality of its audit work papers and the productivity and collaboration with the other assurance teams (i.e., compliance, risk, security) of the company. MetricStream¹ was selected as part partner for this implementation. The platform provided the functionality to quickly evaluate the effectiveness and efficiency of processes, risk and controls.

For assessing the capability of IT processes and the related controls’ design and operational effectiveness, the COBIT® 5 process model was selected and uploaded to the GRC software platform processes universe. The COBIT® process model could be easily mapped to the International Organization for Standardization/International Electrotechnical Commission’s (ISO/IEC’s) ISO/IEC 27001: 2013 information security standard, which is incorporated within the WLA Security Control Standard (WLA-SCS:2016),² a standard widely adopted by lottery companies. Therefore, using both an automated audit management system and a standardized control framework, consistent and repeatable evaluation of the organization’s IT processes’ efficiency, effectiveness, maturity and compliance readiness with the worldwide lottery industry standards could be easily achieved.

WLA Security Control Standard Defined

The security of a lottery plays a critical role in maintaining the confidence and trust of the public in its lottery games. Therefore, it is vital that a lottery organization develops and maintains a visible and documented security environment to achieve and sustain public confidence in its operations.

The WLA-SCS is the lottery sector’s only internationally recognized security standard. The WLA-SCS couples a comprehensive information security management baseline incorporating ISO/IEC 27001:2013, a leading international standard for information security management, with additional lottery-specific security controls.
representing current best practices. The WLA-SCS is designed to assist the lottery sector around the globe in obtaining a level of security controls in line with generally accepted best practices to enable an increased reliance on the integrity of lottery operations. The WLA-SCS specifies the required practices for an effective security management structure by which a lottery can maintain the integrity, availability and confidentiality of information vital to its secure operation.

Implementation Steps

To achieve the goal, the following steps for implementation were planned:

1. Recognize the COBIT 5 processes that are running in the corporate IT environment
4. Upload results to a data visualization platform and produced reports

Step 1: Recognize the COBIT 5 Processes That Are Running in the Corporate IT Environment

In the context of a large-scale business transformation, internal audit facilitated the collection and indexing of company processes, including IT processes, running throughout the organization. The COBIT 5 process model was used as a base model for identifying the organization’s IT core processes regardless of whether they were outsourced or running in-house. Discussions took place between the chief technology officer (CTO) and his team to identify the most important IT processes that would be included in the company’s process model. The result of this exercise has shown that the significant majority of COBIT 5 processes were identified as applicable and were uploaded into the GRC software platform.

Also, during this step, an initial effort was made to rate how the processes affect confidentiality, integrity and availability of information and to estimate the process recovery time objectives (RTOs) and recovery point objectives (RPOs) for the information processed, so as to be reflected in the business continuity and disaster recovery plan later on.

Step 2: Map COBIT 5 Processes to WLA-SCS:2016 and ISO/IEC 27001:2013 Processes and Controls

After identifying the applicable COBIT 5 processes, the next step was to map those processes to a commonly accepted framework regarding gaming operations.

As stated previously, WLA-SCS is a standard that is widely adopted by lottery companies worldwide. The WLA-SCS standard describes both general security controls (covered by ISO/IEC 27001) and specific controls related to the security of the games provided. Using COBIT® 5 for Information Security and, specifically, the referenced table “Mapping of COBIT 5 for Information Security to Related Standards,” one can easily map COBIT 5 processes to ISO/IEC 27001 thus covering the information security requirements of the WLA-SCS:2016. Figure 1 describes the interrelationship of COBIT 5 and WLA-SCS:2016, including what areas can be assessed respectively.
Figure 1—Relationship of COBIT 5 and WLA-SCS:2016

In figure 2, the COBIT 5 coverage of other standards and frameworks is presented, including the ISO/IEC 27000 series.

Figure 2—Mapping of COBIT 5 and the ISO/IEC 27000 Series


For assessing the areas indicated in figure 1, the following methods were used:

- For COBIT 5 processes, ISACA’s Process Assessment Model (PAM), which includes the Process Assessment Model, the Assessor Guide and the PAM tool kit.
- For the ISO/IEC 27001:2013 standard, both the control objectives and controls described in the standard and in ISO/IEC 27002:2013 code of practice.
- For WLA-SCS, the control objectives described in WLA-SCS and relevant guidelines (e.g., Internet Gaming Security Guide, Sports Betting Guideline) published by the WLA.

To facilitate the assessment of COBIT 5 processes, WLA-SCS:2016 and ISO/IEC 27001:2013 controls, the GRC platform was used, providing a set of mechanisms (i.e., surveys and checklists [figure 3]) and standardizing the process.

Surveys and checklists are used in many steps throughout the audit life cycle. Following the preparation of the audit plan and specifically in the planning phase, surveys are used to ask business teams to self-assess the maturity level of the IT processes involved in the auditable area. During the fieldwork phase, specific tasks, based on checklists, are implemented to test the auditable process, risk and related controls design and operational effectiveness. Finally, before audit closure, the processes that are tested by the auditors are rated for their residual risk and maturity level.

Figure 3—Metric Stream GRC Software Internal Audit Checklist Used for COBIT and WLA

Step 4: Upload Results to a Data Visualization Platform and Produce Reports

As described previously, there is a relationship between COBIT 5 and ISO/IEC 27001 and WLA-SCS. Also in COBIT 5 there is a detailed mapping between enterprise goals and IT-related goals and between IT-related goals and IT-related processes.

Figure 4—Sample Spider Diagram of Assessment and Target Values for COBIT Processes
Thus, upon performing the assessment described in step 3, the results are uploaded to a data visualization platform (e.g., SAS Visual Analytics, Excel Power BI). Current vs. target state for all of the previously described areas, and controls related to IT governance, information security and the lottery are visualized and presented through the use of dashboards (figure 4) to provide useful insight to relevant stakeholders.

Conclusion

The use of the COBIT 5 framework along with the ISO 27001 and WLA-SCS standards results in the establishment of a common language for the IT processes between all levels of the organization and a standardized methodology for evaluating the capability of those processes. Also, with the use of a GRC and a data visualization tool, the audit, evaluation and presentation of the IT processes capabilities becomes more efficient.

An important note to keep in mind is that throughout this ongoing effort, small and educated steps are taken rather than large and complicated ones.

Ioannis Panopoulos, CISA, CRISC, CGEIT, CSXF, ISO 27001 LA is group internal audit manager at OPAP S.A., Greece. In the past, he served as head of Information Security and Data Protection at OPAP S.A., senior manager for Eurobank Group and Hellenic Postbank Group and as an IT consultant at various software houses. Panopoulos can be contacted at jpanopoylos@yahoo.com.

Marisa Melliou, CISA, CAML, CCO, CIA, CRMA, CRP, ISO 27001 LA is the director of Group Internal Audit at OPAP S.A., Greece. In the past, she served as chief internal auditor at the Hellenic Financial Stability Fund, associate director at National Bank of Greece, senior manager at Eurobank and acting principle at Deloitte Enterprise Risk and Assurance Services. Melliou can be contacted at melliou.maria@gmail.com.

Endnotes

1 MetricStream, Internal Audit Management Application
3 ISACA, COBIT® 5, USA, 2012
4 Ibid., Appendix C