Using COBIT to Aid in Hospital Risk Management

By Masatoshi Kajimoto, CISA, CRISC

In medical institutions, IT can be a double-edged sword: It can mitigate risk and, yet, be a big risk factor. Without appropriate operational risk management, IT risk management will fail. Based on this author’s experience, COBIT is an essential approach for medical institutions to implement total hospital information systems and manage operational risk. This article will explain how COBIT was utilized for this purpose at Takeda General Hospital, which is located in Aizu-Wakamatsu, Fukushima Prefecture, Japan.

First, a hospital information system (HIS) implementation project process, based on the COBIT approach, was successfully completed and appropriate controls were implemented.

As many COBIT users have realized, identifying the appropriate and necessary COBIT controls can be a high hurdle to overcome. In this case, the organization found that it was easy to identify the necessary COBIT controls after completing the identification of the subjects of control activities.

This article describes this first stage, which is based on the descriptions in the COBIT framework and appendix 1 of COBIT 4.1. Following this guidance, the organization began by utilizing the IT balanced scorecard approach.

The IT balanced scorecard approach works closely with COBIT and is evaluated against the defined business objectives. The COBIT process provides a track from generic business goals to IT goals to IT processes. This results in a set of metric indicators with which to monitor and evaluate IT performance.1

Risk factors in medical institutions include medical (e.g., medical mistakes, hospital infections, errors), financial (e.g., uncollected payments, shortened hospital stays, cost management) and regulatory (e.g., acceptance of interns, electronic statements). To manage the risk and implement a total HIS, a top-down approach is needed. That is where COBIT comes in.

Of course, in Japan, as in most countries, personal data protection is a very important issue, especially in the health care industry, which is governed in this area by Japan’s data protection law as well as an earlier established law relating to medical care record protection. Storing medical care records at external locations is strictly prohibited. Also, medical care record-related systems (network) cannot connect with outside networks (only a closed network is permitted). Furthermore, transfer of data of requests for remuneration for medical treatment can be done only by electronic media, dedicated line or closed network. Therefore, data-protection-related risk is a matter of course in Japan and, thus, was not a key initiative in this project. That said, other health care organizations taking on a similar initiative may need to consider this issue in greater detail during their review of risk and control.

Begin With a Balanced Scorecard

First, the organization strategy was defined, followed by defining the total IT strategy, broken down into great detail. From the first stage, the hospital’s IT risk, including existing risk, risk tolerance levels and risk acceptance levels, was examined. When defining strategy, it is important to keep in mind that a target of value management will support the achievement of business goals; a target of risk management will prevent the achievement of business goals. Using a traditional balanced scorecard
approach, the HIS implementation steering committee, which was established by the hospital president, discussed risk factors with the hospital’s senior management.

The vision and mission statement of senior management are very important in a total HIS, as in any industry. If a total HIS cannot support the top management’s vision and mission statement, the system is of no use. The team determined the following goals for the total HIS, in keeping with top management’s vision:

- Maintain a high level of security and personal information data protection.
- Raise and maintain a high level of medical services.
- Minimize medical mistakes (malpractices).
- Rapidly respond to the medical needs of the community.
- Improve information sharing between the hospital and the community.
- Raise the staff’s skills and knowledge.
- Identify and address new challenges.
- Implement cooperation among each facility.
- Establish total support systems for health care, treatments and nursing care.
- Establish a better environment for doctors’ research activities, and improve medical care in the hospital and related facilities.

Strategic Alignment With Customer Satisfaction

For a hospital, the customers are the patients as well as the communities it serves. The next step was to define customer satisfaction performance indices, or value and risk scales. If the established level is higher than the current level, it will be value creation. If the established level is lower than the current level, risk may be actualized. The team identified the following areas to evaluate on value and risk scales:

- **Improvement of patient satisfaction**—Quick response, shortening of period of treatment, wide selection of methods of treatment, completeness of informed consent forms and better disclosure of information
- **Improvement of cooperation between hospitals and clinics in the same community (medical care zone)**—Quick information sharing, an excellent medical information center, cooperation with the local government where necessary, adherence to the local community’s standards of health care, and improved response from the emergency medical service
- **Improvement of the general public’s satisfaction**—Better disclosure of medical information and better services for healthy people to maintain their health

Strategic Alignment With Finance

With regard to financial issues, the team identified the following areas to evaluate on value and risk scales:

- **Growth**—Accuracy of the request to the health insurance society for remuneration for medical treatments, improvement of profit and appropriate capture of billable medical practice items
- **Profitability**—Effect of cost-reduction activities and capture of information about items that can be cost analyzed
- **Liquidity**—Analysis of factors that determine cash flow worth and better control of equipment and facilities that are counted fixed assets
- **Stability**—Better control of personnel expenses (labor cost)

Strategic Alignment With the Internal Process

When considering the internal process, there are many risk factors and hurdles. Problems related to personally identifiable data (PID) are also hidden here. The team considered:

- **Improvement of the quality of medical service**—Substantial standardized medical treatments, substantial clinical paths and application of them, and substantial medical research and study environments for doctors
- **Medical risk management**—Tracking of medical practices, detailed tracking of medicines from procurement to administration, minimizing medical mistakes (e.g., errors, malpractices) and problem analysis
- **Improvement of business process**—Simplification and speed-up of processes and separation of professional processes and standardized processes
- **Utilization of information**—Expansion of information and knowledge sharing environment (based on “need to know, need to do”) and promotion of end-user computing (EUC) utilization

Learning and Growth
The last BSC area involves “what we can learn and how we can grow.” This area may appear easy, but there can be profound problems. New roles and responsibilities require staffing, and there can be apprehension from personnel (e.g., “This is not my job. Someone else should do this.”). This area strongly depends on senior management’s intentions. And, all staff must remain knowledgeable about medical treatments and regulatory issues. The team focused on:

- **Improvement of professionalism of staff**—Professional knowledge sharing and electronic information gathering and analysis environment
- **Optimization of roles and responsibilities**—Support and optimal roles and responsibilities assignment, and appropriate information security environment
- **Continuing education**—Status of knowledge management implementation, sharing know-how within the hospital, increasing learning opportunities, and flexibility and quick response to environmental changes

### Risk Management

To establish appropriate risk management, the preparation phase is very important. The following activities are indispensable:

- **Standardization of wording (name or abbreviation of disease)**—Medical wording was different for each medical department. For example, “HT” could mean “hypertension” (high blood pressure) or “hypotension” (low blood pressure).
- **Change to globally standardized disease name**—This seems easy, but adjustments among many medical divisions can be very difficult. Using a globally recognized standard is essential.
- **Standardization of medical process**—Each medical department operated independently and used its own customized medical process. All need to use a standardized process.
- **Unification of patient case records**—At first, the team found that each medical department managed its own medical record for each patient, creating too many patient case records for one patient. The record should be unified.
- **Standardization of medicine name**—There are different medicines for the same disease and medicines of very similar names. For example, for breast cancer, there is Taxol (paclitaxel) and Taxotere (docataxel). Standardization will reduce confusion.

If standardization of wording is not performed, the dictionary of electronic medical chart systems cannot be implemented, and can become the cause of medical errors. In which case, disease name and appropriate care does not correctly correspond in the system. If standardization of medical processes is not performed, the HIS becomes very complicated and needs many customizations. Such system will be costly and become the cause of human errors. These activities are effectively controlled by PO6, PO7, PO9 and the application controls in COBIT.

### Understanding IT

Of course, IT can mitigate risk, such as the interdependency check of diseases, contraindication of medicines, customer/patient satisfaction, medical mistakes, and tracking of wrong medicine and operating costs. But what about other IT risk factors? For example, can terminals (PCs) be sterilized in boiling water? (Only recently have some medical vendors begun providing terminals that can be sterilized.) If a terminal is contaminated by MRSA, what will happen? Electromagnetic Wave (Wi-Fi) may interfere with delicate medical equipment. If local area network (LAN) cables are used for a terminal, such cables may be contaminated. If a power failure occurs, what will happen? Stealing of paper-based patient records is very difficult, but electronic medical chart data are easy to steal for internal (authorized) personnel.

Further, if a doctor cannot utilize a PC quickly, what will happen? If a doctor inputs a wrong disease name or other data, what will happen? If an appropriate recovery process of the system does not exist, what will happen? For IT, 24 hours per day, 365 days per year, operational risk management is a matter of fact.

### Conclusion

IT risk and operational risk have interdependencies. And, IT can be a double-edged sword—mitigating risk and, yet, being a risk factor. IT, business processes and human factors all must be considered at the same time. Additionally, if one wants to increase value, risk will increase. If a sound risk management environment is established, value will be created. Separating risk and value is impossible.

This article described the identification of subjects that need appropriate controls; the next phase is identification of controls based on COBIT. Please watch for a future article, expected in volume 2, 2012, of COBIT Focus, covering this phase of the project.

**Masatoshi Kajimoto, CISA, CRISC**

Is an IT auditor and independent consultant providing services in BPR, HRM, IT governance and IT-related risk management
for educational, medical and financial institutions. He currently serves as technical advisor for the Ministry of Internal Affairs & Communications (Japanese government). He is a director of the ISACA Tokyo Chapter and is a cofounder and executive director of ITGI Japan. He also serves on ISACA’s GRA Subcommittee Area 1 and is a member of the GRA Committee.

Endnote

1 www.slideshare.net/MichaelSim/cobit-val-it-balanced-scorecards-presentation