Organizations maintain their operations with the help of processes that differ according to their organizational structure, business objectives and working styles. A process determines and manages numerous linked activities within an organization to help ensure that the organization functions effectively. It is “an activity or set of activities using resources, and managed in order to enable the transformation of inputs into outputs.” Furthermore, processes for managing IT operations should be formed because IT is a part of every business process.

The processes described in this article were identified as critical from the viewpoint of using confidential information in business operations. These processes have been chosen by taking into account the requirements of well-known IT frameworks and standards that provide a general understanding of the processes that need to be established within organizations. COBIT®, the Project Management Body of Knowledge (PMBOK), the Capability Maturity Model Integration (CMMI), the IT Infrastructure Library (ITIL), ISO 27001, The Open Group Architecture Framework (TOGAF) and ISO 9001:2008 were considered in preparation of these critical processes. The chosen processes are also included in the Certified in Risk and Information Systems Control™ (CRISC™) Review Manual.

In COBIT® 5, the concept of critical IT processes is stressed and required in processes DSS01.02 (integration of critical internal IT management processes with those of outsourced service providers) and MEA01 (percent of critical processes monitored). In MEA02, the percent of critical business processes covered by risk assessment is defined as a process performance metric.

While these methods often differ based on the organization’s approach to problem solving and its targeted audience, the most important common issues were taken into consideration in order to develop this list of critical IS processes (figure 1).

**Figure 1—Presence of Critical Processes in Key Frameworks/Standards**

<table>
<thead>
<tr>
<th>IS Process Name</th>
<th>COBIT</th>
<th>PMBOK</th>
<th>CMMI</th>
<th>ITIL</th>
<th>ISO 270001</th>
<th>TOGAF</th>
<th>ISO 9001:2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determining the IT strategy</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Project and program management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Change management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Third-party service management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Continuous service assurance</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Information security management</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Configuration management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Problem management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Data management</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Physical environment management</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>IT operations management</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

(+ Related process is included in the standard/framework. (-) Related process is not included in the standard/framework.)
DETERMINING IT STRATEGY
Strategy is the first step in determining the organization’s direction, and “technology has become so embedded in the internal functions and the external value propositions of modern organizations that it is impossible to execute strategy in any organization without it.” The IT strategy should be in line with the organization’s objectives in order to support the business in achieving its strategic goals. There should be a clear strategy for information transfer from organization management to IT management, and mechanisms should be in place to align with these strategies. There should be no discrepancies between the organization and IT strategy; any discrepancies here would conflict with the aim of advancing strategic goals. A strategy plan should be developed and regularly updated for compliance with changing business needs and objectives. This process should also comply with any new competitive changes in the environment and should provide for updating the strategy according to these changes to catch up with the evolving environment.

THE PROJECT AND PROGRAM MANAGEMENT PROCESS
Business objectives can be achieved only by following the business strategy. “If IT is to deliver the services that a business needs now and in the future, it has to be managed by the business as a whole.” This can be done by allocating resources and budget in line with business priorities. Doing the right projects with the right prioritization is significant; therefore, project and program management plays a crucial role. Project planning, relationships among projects, resource planning and project budgeting should be established according to business priorities. In addition, requirements planning, risk management, testing, quality management and stakeholder approval phases have critical importance on the project’s success. Project success should be reviewed to ensure that value is delivered to the organization.

THE CHANGE MANAGEMENT PROCESS
Since business environments undergo rapid changes, organizations are expected to adapt and, thus, must reevaluate business goals and direction. This makes the change management process crucial since keeping up with these changes carries new risk and opportunities to the organization. “Competitive pressures, rising expectations from global customers and the emergence of newer technologies, especially in the area of telecommunication, have accelerated the process of change management.” In order to manage changes to take advantage of opportunities in business and to minimize the related risk, the change management process should involve a number of phases: monitoring and taking change requests, prioritizing them, evaluating the change impact, taking the appropriate stakeholder approvals, tracking the status of the changes to ensure that they are done as planned, and reporting.

THE THIRD-PARTY SERVICE MANAGEMENT PROCESS
As organizations focus on their primary service area, they may get some outsource support for their operations. This is common in IT since IT is an integral part of business operation support. Third-party services directly affect the organization’s business operations, and management of these services is significant. Every detail about the service requirements, roles and responsibilities, communications, legal obligations, payment, support, and cancellation should be determined and written into the contract. This process should also include compliance monitoring of third-party contracts. “Properly constituted organizations have the capacity to enter into contracts with one another, and many legal endeavors go into working out the terms of the contract, as well as assessing how its terms are complied with during the duration of the contract.”

THE CONTINUOUS SERVICE ASSURANCE PROCESS
“The confidentiality, integrity and availability of information systems must be ensured to protect the business from the risk relating to IT.” Organizations may face some disruptions such as natural disasters or service outages. Organizations should take precautions so that these disruptions are not reflected on their customers and service continues. This process determines critical business processes and ensures the continuous backup to an alternative site away from the risk associated with the main site.

Roles and responsibilities are important in the event of a disruption; all critical personnel should know how to act. Manuals and communication information should be
in place at the staff members’ homes and at the alternative site. Continuity should be periodically tested to ensure its applicability. The business continuity plan should be documented clearly and updated periodically. This process is significant since organizations are expected to serve the customer continuously and to cope with such disruptions.

THE INFORMATION SECURITY MANAGEMENT PROCESS
Information is the most important asset of the organizations; it is indispensable to its operation. There are remarkable issues to consider in using IT as a support for business operations. IT assets should be protected against vulnerabilities and incidents in order to minimize the business impact of damaged security. Information systems security management essentially belongs to risk management, handling the threat of attacks on the system and dealing with the threat posed by vulnerabilities.

This process should include determining security roles and responsibilities, information security rules, procedures, policies, and standards. Monitoring noncompliance to security policies and related rules and periodically testing to ensure the safety of information systems should be established in the organization. Corrective and improvement actions should be maintained to ensure that risk is minimized. Security management should be performed effectively to ensure the protection of information assets and continuity of services. To accomplish this difficult task in today’s risky technology environment, new risk factors and threats should be continuously reviewed and appropriate mechanisms should be established rapidly.

THE CONFIGURATION MANAGEMENT PROCESS
Providing for system availability, production issue management and recovery from erroneous operations is important for business continuity, safety and customer satisfaction. The configuration management process aims to accurately and completely configure inventory. Backing up the configuration information is a part of this process as it helps return business to its original or previous state when a problem occurs. Integrity of these configurations should be monitored and tested periodically as part of this process.

THE PROBLEM MANAGEMENT PROCESS
It is common to face problems in ongoing business operations related to IT. Organizations establish problem management processes to return to normal operation of business activities as soon as they can. Recognizing the problem, communicating the problem to appropriate parties, conducting a root-cause analysis, determining the solution, undertaking the appropriate stakeholder approval for solutions, resolving the problem and monitoring the status of the problem are important stages of the process. Documentation and reporting for knowledge sharing are also significant for this process in order to accelerate the resolution of known problems.

Periodic analysis of the problems encountered can result in process improvements that can improve the organization’s ability to perform business activities.

THE DATA MANAGEMENT PROCESS
An entity’s information assets constitute a significant portion of the entity’s market value, making this a key enterprise asset that needs to be governed effectively. Business operation’s quality is strictly related to the timeliness, availability and quality of business data. Accuracy, consistency, completeness, confidentiality, integrity and availability are desired characteristics of data for business use. To accomplish this task, it is important to establish a data management process. This process should involve determining the data storage and retention requirements with business management, establishing and maintaining a media library, protecting data, backing up data, and restoring and disposing of data and sensitive media.

THE PHYSICAL ENVIRONMENT MANAGEMENT PROCESS
Physical facilities should be managed to protect computer and related equipment. Appropriate physical conditions should be selected for business continuity. Computer and related equipment should operate effectively in the selected environment. Establishing and maintaining this process could help organizations to minimize damage to the physical facilities and, therefore, minimize interruption to business operations. Protection of the physical facilities includes

Discuss and collaborate on change management, service management and information security management in the Knowledge Center.

www.isaca.org/knowledgecenter
protection of physical facility staff. This process also reduces the organization’s resource allocation for maintenance.

**THE IT OPERATIONS MANAGEMENT PROCESS**

Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process is crucial since operating policies and procedures need to be defined and standardized to help safeguard the continuation of business activities. Performance monitoring for infrastructure and related technology should be established, and information mechanisms for the detected events should be set up. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.

**CONCLUSION**

Determining critical IS processes is crucial in order for organizations to prioritize their efforts toward achieving business objectives. Perhaps the most important improvement will be the extension of the domain and range of these processes from the IT arena into corporate operations.

When classifying the scope of operations, the domain of these critical processes could be decomposed; the components of the domain might facilitate the application of these processes in the everyday life of a business. A possible partition may be the three pillars: organizational, regulation and technical, which were first defined as pillars of IT and later generalized to pillars of operations.

These critical information processes can also be used as a reference for MEA01 and MEA02 processes in COBIT 5 to prioritize critical information systems processes.

**ACKNOWLEDGEMENTS**

The authors would like to thank Katalin Szenes, Ph.D., Obuda University, for her valuable comments.

---

**ENDNOTES**

2. Business objectives can be achieved only by following the business strategy. ISACA, COBIT 5, 2012, www.isaca.org/cobit
3. In COBIT® 4.1, the concept of critical IT processes is stressed and required under many control objectives, including PO4.11 (importance of segregation of duties), PO7.5 (dependence upon individuals for critical processes) and ME2.2 (managerial oversight for critical processes).
13. Ibid.