

Development and Acquisition

This rating reflects an organization's ability to identify, acquire, install, and maintain appropriate information technology solutions. Management practices may need to address all or parts of the business process for implementing any kind of change to the hardware or software used. These business processes include an institution's or service provider's purchase of hardware or software, development and programming performed by the institution or service provider, purchase of services from independent vendors or affiliated data centers, or a combination of these activities. The business process is defined as all phases taken to implement a change including researching alternatives available, choosing an appropriate option for the organization as a whole, converting to the new system, or integrating the new system with existing systems. This rating reflects the adequacy of the institution's systems development methodology and related risk technology. This rating also reflects the board's and management's ability to enhance and replace information technology prudently in a controlled environment. The performance of systems development and acquisition and related risk management practice is rated based upon an assessment of factors such as:

- The level and quality of oversight and support of systems development and acquisition activities by senior management and the board of directors;
- The adequacy of the organizational and management structures to establish accountability and responsibility for IT systems and technology initiatives;
- The volume, nature, and extent of risk exposure to the financial institution in the area of systems development and acquisition;
- The adequacy of the institution's system development life cycle (SDLC) and programming standards;
- The quality of project management programs and practices which are followed by developers, operators, executive management/owners, independent vendors or affiliated servicers, and end users;
- The independence of the quality assurance function and the adequacy of controls over program changes;
- The quality and thoroughness of system documentation;
- The integrity and security of the network, system, and application software;
- The development of information technology solutions that meet the needs of end users; and
- The extent of end user involvement in the system development process.

In addition to the above, factors such as the following are included in the assessment of development and acquisition at service providers:

- The quality of software releases and documentation; and
- The adequacy of training provided to clients.

Ratings

A rating of 1 indicates strong systems development, acquisition, implementation, and change management performance. Management and the board routinely demonstrate successfully the ability

to identify and implement appropriate IT solutions while effectively managing risk. Project management techniques and the SDLC are fully effective and supported by written policies, procedures, and project controls that consistently result in timely and efficient project completion. An independent quality assurance function provides strong controls over testing and program change management. Technology solutions consistently meet end-user needs. No significant weaknesses or problems exist.

A rating of 2 indicates satisfactory systems development, acquisition, implementation, and change management performance. Management and the board frequently demonstrate the ability to identify and implement appropriate IT solutions while managing risk. Project management and the SDLC are generally effective; however, weaknesses may exist that result in minor project delays or cost overruns. An independent quality assurance function provides adequate supervision of testing and program change management, but minor weaknesses may exist. Technology solutions meet end-user needs. However, minor enhancements may be necessary to meet original user expectations. Weaknesses may exist; however, they are not significant and they are easily corrected in the normal course of business.

A rating of 3 indicates less than satisfactory systems development, acquisition, implementation, and change management performance. Management and the board may often be unsuccessful in identifying and implementing appropriate IT solutions; therefore, unwarranted risk exposure may exist. Project management techniques and the SDLC are weak and may result in frequent project delays, backlogs or significant cost overruns. The quality assurance function may not be independent of the programming function, which may adversely impact the integrity of testing, and program change management. Technology solutions generally meet end-user needs, but often require an inordinate level of change after implementation. Because of weaknesses, significant problems may arise that could result in disruption to operations or significant losses.

A rating of 4 indicates deficient systems development, acquisition, implementation, and change management performance. Management and the board may be unable to identify and implement appropriate IT solutions and do not effectively manage risk. Project management techniques and the SDLC are ineffective and may result in severe project delays and cost overruns. The quality assurance function is not fully effective and may not provide independent or comprehensive review of testing controls or program change management. Technology solutions may not meet the critical needs of the organization. Problems and significant risks exist that require immediate action by the board and management to preserve the soundness of the institution.

A rating of 5 indicates critically deficient systems development, acquisition, implementation, and change-management performance. Management and the board appear to be incapable of identifying and implementing appropriate information technology solutions. If they exist, project management techniques and the SDLC are critically deficient and provide little or no direction for development of systems or technology projects. The quality assurance function is severely deficient or not present and unidentified problems in testing and program change management have caused significant IT risks. Technology solutions do not meet the needs of the organization. Serious problems and significant risks exist that raise concern for the financial institution or service provider's ongoing viability.