

Management

This rating reflects the abilities of the board and management as they apply to all aspects of IT acquisition, development, and operations. Management practices may need to address some or all of the following IT-related risks: strategic planning, quality assurance, project management, risk assessment, infrastructure and architecture, end-user computing, contract administration of third-party service providers, organization and human resources, and regulatory and legal compliance. Generally, directors need not be actively involved in day-to-day operations; however, they must provide clear guidance regarding acceptable risk exposure levels and ensure that appropriate policies, procedures, and practices have been established. Sound management practices are demonstrated through active oversight by the board of directors and management, competent personnel, sound IT plans, adequate policies and standards, an effective control environment, and risk monitoring. This rating should reflect the ability of the board and management as it applies to all aspects of IT operations. The performance of management and the quality of risk management are rated based upon an assessment of factors such as:

- The level and quality of oversight and support of the IT activities by the board of directors and management;
- The ability of management to plan for and initiate new activities or products in response to information needs and to address risks that may arise from changing business conditions;
- The ability of management to provide information reports necessary for informed planning and decision making in an effective and efficient manner;
- The adequacy of, and conformance with, internal policies and controls addressing the IT operations and risks of significant business activities;
- The effectiveness of risk monitoring systems;
- The timeliness of corrective action for reported and known problems;
- The level of awareness of and compliance with laws and regulations;
- The level of planning for management succession;
- The ability of management to monitor the services delivered and to measure the organization's progress toward identified goals in an effective and efficient manner;
- The adequacy of contracts and management's ability to monitor relationships with third-party servicers;
- The adequacy of strategic planning and risk management practices to identify, measure, monitor, and control risks, including management's ability to perform self-assessments; and
- The ability of management to identify, measure, monitor, and control risks and to address emerging information technology needs and solutions.

In addition to the above, factors such as the following are included in the assessment of management at servicer providers:

- The financial condition and ongoing viability of the entity;
- The impact of external and internal trends and other factors on the ability of the entity to support continued servicing of client financial institutions; and
- The propriety of contractual terms and plans.

Ratings

A rating of 1 indicates strong performance by management and the board. Effective risk management practices are in place to guide IT activities, and risks are consistently and effectively identified, measured, controlled, and monitored. Management immediately resolves audit and regulatory concerns to ensure sound operations. Written technology plans, policies and procedures, and standards are thorough and properly reflect the complexity of the IT environment. They have been formally adopted, communicated, and enforced throughout the organization. IT systems provide accurate, timely reports to management. These reports serve as the basis of major decisions and as an effective performance-monitoring tool. Outsourcing arrangements are based on comprehensive planning; routine management supervision sustains an appropriate level of control over vendor contracts, performance, and services provided. Management and the board have demonstrated the ability to promptly and successfully address existing IT problems and potential risks.

A rating of 2 indicates satisfactory performance by management and the board. Adequate risk management practices are in place and guide IT activities. Significant IT risks are identified, measured, monitored, and controlled; however, risk management processes may be less structured or inconsistently applied and modest weaknesses exist. Management routinely resolves audit and regulatory concerns to ensure effective and sound operations; however, corrective actions may not always be implemented in a timely manner. Technology plans, policies, procedures, and standards are adequate and are formally adopted. However, minor weaknesses may exist in management's ability to communicate and enforce them throughout the organization. IT systems provide quality reports to management that serve as a basis for major decisions and a tool for performance planning and monitoring. Isolated or temporary problems with timeliness, accuracy, or consistency of reports may exist. Outsourcing arrangements are adequately planned and controlled by management, and provide for a general understanding of vendor contracts, performance standards, and services provided. Management and the board have demonstrated the ability to address existing IT problems and risks successfully.

A rating of 3 indicates less than satisfactory performance by management and the board. Risk management practices may be weak and offer limited guidance for IT activities. Most IT risks are generally identified; however, processes to measure and monitor risk may be flawed. As a result, management's ability to control risk is less than satisfactory. Regulatory and audit concerns may be addressed, but time frames are often excessive and the corrective action taken may be inappropriate. Management may be unwilling or incapable of addressing deficiencies. Technology plans, policies, procedures, and standards exist, but may be incomplete. They may not be formally adopted, effectively communicated, or enforced throughout the organization. IT systems provide requested reports to management, but periodic problems with accuracy, consistency, and timeliness lessen the reliability and usefulness of reports and may adversely affect decision making and performance monitoring. Outsourcing arrangements may be entered into without thorough planning. Management may provide only cursory supervision that limits its understanding of vendor contracts, performance standards, and services provided. Management and the board may not be capable of addressing existing IT problems and risks, as evidenced by untimely corrective actions for outstanding IT problems.

A rating of 4 indicates deficient performance by management and the board. Risk management practices are inadequate and do not provide sufficient guidance for IT activities. Critical IT risks are not properly identified, and processes to measure and monitor risks are not properly identified, and processes to measure and monitor risks are deficient. As a result, management may not be aware of and is unable to control risks. Management may be unwilling or incapable of addressing audit and regulatory deficiencies in an effective and timely manner. Technology plans, policies and procedures, and standards are inadequate, have not been formally adopted or effectively communicated throughout the organization, and management does not effectively enforce them. IT systems do not routinely provide management with accurate, consistent, and reliable reports, thus contributing to ineffective performance monitoring or flawed decision-making. Outstanding arrangements may be entered into without planning or analysis, and management may provide little or no supervision of vendor contracts, performance standards, or services provided. Management and the board are unable to address existing IT problems and risks, as evidenced by ineffective actions and longstanding IT weaknesses. Strengthening of management and its processes is necessary. The financial condition of the service provider may threaten its viability.

A rating of 5 indicates critically deficient performance by management and the board. Risk management practices are severely flawed and provide inadequate guidance for IT activities. Critical IT risks are not identified, and processes to measure and monitor risks do not exist, or are not effective. Management's inability to control risk may threaten the continued viability of the institution or service provider. Management is unable or unwilling to correct audit and regulatory identified deficiencies and immediate action by the board is required to preserve the viability of the institution or service provider. If they exist, technology plans, policies, procedures, and standards are critically deficient. Because of systemic problems, IT systems do not produce management reports that are accurate, timely, or relevant. Outsourcing arrangements may have been entered into without management planning or analysis, resulting in significant losses to the financial institution or ineffective vendor services. The financial condition of the service provider presents an imminent threat to its viability.