FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

Uniform Rating System for Information Technology

AGENCY: Federal Financial Institutions Examination Council.

ACTION: Notice and request for comment.

SUMMARY: The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) (collectively referred to as the federal supervisory agencies), under the auspices of the Federal Financial Institutions Examination Council (FFIEC) request comment on proposed changes to the Uniform Interagency Rating System for Data Processing Operations, commonly referred to as the Information Systems rating system. The proposed revisions change the name of the rating system to the Uniform Rating System for Information Technology (URSIT) and reflect changes that have occurred in the data processing services industry and in supervisory policies and procedures since the rating system was first adopted in 1978. The proposed changes revise the numerical ratings to conform to the language and tone of the Uniform Financial Institution Rating System (UFIRS) rating definitions, commonly referred to as the CAMELS rating system; reformat and clarify the component rating descriptions; emphasize the quality of risk management processes in each of the rating components; add two new component categories, Development and Acquisition, and Support and Delivery as replacements for Systems Development and Programming, and Operations; and explicitly identify the risk types that are considered in assigning component ratings. After reviewing public comments, the FFIEC intends to make appropriate additional changes to the revised URSIT, if necessary, and adopt a final information technology rating system.

The *term financial institution* refers to those FDIC insured depository institutions whose primary Federal supervisory agency is represented on the FFIEC, Bank Holding Companies, Branches and Agencies of Foreign Banking Organizations, and Thrifts. The term ''service provider'' refers to organizations that provide data processing services to financial institutions. Uninsured trust companies that are chartered by the OCC, members of the Federal Reserve System, or subsidiaries of registered bank holding companies or insured depository institutions are also covered by this action.

DATES: Comments must be received by August 10, 1998.

ADDRESSES: Comments should be sent to Keith Todd, Acting Executive Secretary, Federal Financial Institutions Examination Council, 2100 Pennsylvania Avenue, NW, Suite 200, Washington, DC 20037 (Fax number: (202) 634–6556). Comments will be available for public inspection during regular business hours at the above address. Appointments to inspect comments are encouraged and can be arranged by calling the FFIEC at (202) 634–6526.

FOR FURTHER INFORMATION CONTACT:

FRB: Charles Blaine Jones, Supervisory EDP Analyst, Specialized Activities, (202) 452–3759, Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System, Mail Stop 182, 20th and C Streets, NW, Washington, DC 20551

FDIC: Stephen A. White, Review Examiner (Information Systems), (202) 898–6923, Division of Supervision, Federal Deposit Insurance Corporation, Room F–6010, 550 17th Street, NW, Washington, DC 20429

OCC: Norine Richards, National Bank Examiner, (202) 874–4924, Bank Technology Unit, Office of the Comptroller of the Currency, Mail Stop 7–9, 250 E Street, SW, Washington, D.C. 20219

OTS: Jennifer Dickerson, Program Manager, Information System Examinations, Compliance Policy, (202) 906–5631, Office of Thrift Supervision, 1700 G Street, NW, Washington, D.C. 20552

SUPPLEMENTARY INFORMATION:

Background Information

The Uniform Interagency Rating System for Data Processing Operations is an internal rating system used by federal and state regulators to assess uniformly financial institution and service provider risks introduced by information technology and for identifying those institutions and service providers requiring special supervisory attention. The current rating system was adopted in 1978 by the OCC, OTS, FDIC and FRB, and is commonly referred to as the IS rating system. Each financial institution or service provider is assigned a composite rating based on an evaluation and rating of four essential components of an institution's information technology. These components address the following: the adequacy of the information technology audit function; the capability of information technology management; the adequacy of systems development and programming, and the quality, reliability, availability and integrity of information technology operations. Both the composite and component ratings are assigned on a ''1'' to ''5'' numerical scale. A ''1'' indicates the strongest performance and management practices, and the least degree of supervisory concern, while a ''5'' indicates the weakest performance and management practices and, therefore, the highest degree of supervisory concern.

The composite rating reflects the overall condition of an institution's or service provider's information technology function. The composite ratings are used by the federal and state supervisory agencies to monitor aggregate trends in the overall administration of information technology.

The IS rating system has proven to be an effective means for the federal and state supervisory agencies to determine the condition of an institution's or service provider's information technology function. A number of changes, however, have occurred in information technology and in supervisory policies and procedures since the rating system was first adopted. The FFIEC's Task Force on Supervision has reviewed the existing rating system in light of these industry trends. The Task Force has concluded that the current rating system framework should be modified to provide a more effective vehicle for summarizing conclusions about the condition of an institution's or service provider's information technology function. As a result, the FFIEC proposes to retain the basic rating framework, and the revised rating system will continue to assign a composite rating based on an evaluation and rating of essential components of an institution's or service provider's information technology function. However, the FFIEC proposes certain enhancements to the rating system.

Discussion of Proposed Changes to the Rating System

1. Structure and Format

The FFIEC proposes to enhance and clarify the component rating descriptions by reformatting each component into three distinct sections. These sections are: (a) An introductory paragraph discussing in general terms the areas to be considered when rating each component; (b) a bullet-style listing of the specific evaluation factors

to be considered when assigning the component rating; and, (c) a brief qualitative description of the five rating grades that can be assigned to a particular component.

2. Alignment of Composite and Component Ratings

The FFIEC proposes changes to revise the definitions of the composite and component ratings to align the URSIT rating definitions more closely with the language and tone of the UFIRS rating definitions. For example, under the current rating system a composite ''3'' rated information technology function has performance that is flawed to some degree and is considered to be of below average quality, while under the UFIRS a composite ''3'' rated bank or service provider exhibits some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe. The proposed revision brings the URSIT in line with the language and tone of the UFIRS.

3. Component Reorganization

The current rating system has four components: (1) Audit; (2) Management; (3) Systems Development and Programming; and (4) Operations. The FFIEC is proposing to replace the current ''Systems Development and Programming'' and ''Operations'' components with two new component categories, ''Development and Acquisition'', and ''Support and Delivery''. The new components will address all areas assessed in the current Systems Development and Programming and Operations components. In addition, the new components will provide a more effective framework for the risks encountered in distributed processing environments and emerging technology.

4. Composite Rating Definitions

The FFIEC is proposing changes in the composite rating definitions to parallel the changes in the component rating descriptions. Under the FFIEC's proposal, the revised composite rating definitions would contain an explicit reference to the quality of overall risk management practices. The basic context of the existing composite rating definitions is being retained. The composite rating would continue to be based on a careful evaluation of an institution's or service provider's ability to monitor, manage, develop, acquire, support and deliver information technology services.

5. Risk Management

The FFIEC is proposing that the revised rating system emphasize risk management processes. Changes in information technology have broadened the range of products and services offered. These trends reinforce the importance of institutions having sound risk management processes. Accordingly, the revised rating system would contain language in each of the components emphasizing the consideration of processes to identify, measure, monitor, and control risks.

Request for Comments

The FFIEC requests comment on the proposed revisions to the URSIT (''the proposal''). In particular, the FFIEC invites comments on the following questions:

1. Does the proposal capture the essential risk areas of information technology?
2. Does the proposal adequately address distributed processing environments, as well as centralized processing environments?
3. Does the proposal adequately address risks to financial institutions that process their data in-house as well as to data processing service providers?
4. Are the definitions for the individual components and the composite numerical ratings in the proposal consistent with the language and tone of the UFIRS definitions?
5. Are there any components which should be added to or deleted from the proposal?
6. Given the trend toward the integration of safety and soundness and information technology examination functions by the federal supervisory agencies, does a separate rating system for information technology continue to be useful?

Text of the Revised Uniform Rating System for Information Technology

Uniform Rating System for Information Technology

Introduction

The quality, reliability, and integrity of a financial institution's or service provider's information technology (IT) affect all aspects of its performance. An assessment of the technology risk management framework is necessary whether or not the institution itself or a third-party service provider manages these operations. The Uniform Rating System for Information Technology (URSIT) is an internal rating system used by federal and state regulators to uniformly assess financial institution and service provider risks introduced by IT. It also allows the regulators to identify those insured institutions and service providers whose information technology risk exposure requires special supervisory attention. The rating system includes component and composite rating descriptions and the explicit identification of risks and assessment factors that might be considered in assigning component ratings. Additionally, information technology can affect the risks associated with financial institutions. For each IT rating component the effect on credit, operational, market, reputation, strategic, and compliance risks should be considered.

The purpose of the rating system is to identify those entities whose risk exposure requires special supervisory attention. This rating system assists examiners in making an assessment of risk and compiling examination findings. However, the rating system does not drive the scope of an examination. Examiners should use the rating system to help evaluate the entity's overall risk exposure, and determine the degree of supervisory attention believed necessary to ensure that weaknesses are addressed and that risk is properly managed.

Overview

The URSIT is based on a risk evaluation of four critical components: Audit, Management, Development and Acquisition, and Support and Delivery (AMDS). These components, when combined, are used to assess the overall performance of IT within an organization. Examiners evaluate the functions identified within each component to assess the institution's ability to identify, measure, monitor and control information technology risks. Each organization examined for IT is assigned a summary or composite rating based on the overall results of the evaluation. The IT composite rating and each component rating are based on a scale of ''1'' through ''5'' in ascending order of supervisory concern; ''1'' representing the highest rating and least degree of concern, and ''5'' representing the lowest rating and highest degree of concern.

The first step in developing an IT composite rating for an organization is the assignment of a performance rating to the individual AMDS components. The evaluation of each of these components, their interrelationships, and relative importance is the basis for the composite rating. The composite rating is derived by making a qualitative summarization of all of the AMDS components. A direct relationship exists between the composite rating and the individual AMDS component

performance ratings. However, the composite rating is not an arithmetic average of the individual components. An arithmetic approach does not reflect the actual condition of IT when using a risk-focused approach. A poor rating in one component may heavily influence the overall composite rating for an institution. For example, if the audit function is viewed as inadequate, the overall integrity of the IT systems is not readily verifiable. Thus, a composite rating of less than satisfactory (''3''–''5'') would normally be appropriate.

A principal purpose of the composite rating is to identify those financial institutions and service providers that pose an inordinate amount of information technology risk and merit special supervisory attention. Thus, individual risk exposures that more explicitly affect the viability of the organization and/or its customers should be given more weight in the composite rating.

The following two sections contain the URSIT composite rating definitions, the assessment factors, and definitions for the four component ratings. These assessment factors and definitions outline various IT functions and controls that may be evaluated as part of the examination.

Composite Ratings [1]

Composite 1

Financial institutions and service providers rated composite ''1'' exhibit strong performance in every respect. Weaknesses in IT are minor in nature and are easily corrected during the normal course of business. Risk management processes provide a comprehensive program to identify and monitor risk relative to the size, complexity and risk profile of the entity. Strategic plans are well defined and fully integrated throughout the organization. This allows management to quickly adapt to changing market, business and technology needs of the entity. Management identifies weaknesses promptly and takes appropriate corrective action to resolve internal audit and regulatory concerns. The financial condition of the service provider is strong and overall performance shows no cause for supervisory concern.

Composite 2

Financial institutions and service providers with composite rating of ''2'' exhibit safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes or system development. Generally, senior management corrects weaknesses in the normal course of business. Risk management processes adequately identify and monitor risk relative to the size, complexity and risk profile of the entity. Strategic plans are defined but may require clarification, better coordination or improved communication throughout the organization. As a result, management anticipates, but responds less quickly, to changes in market, business, and technological needs of the entity. Management normally identifies weaknesses and takes appropriate corrective action. However, greater reliance is placed on audit and regulatory intervention to identify and resolve concerns. The financial condition of the service provider is acceptable and while internal control weaknesses may exist, there are no significant supervisory concerns. As a result, supervisory action is limited.

Composite 3

Financial institutions and service providers rated composite ''3'' exhibit some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe. If weaknesses persist further deterioration in the condition and performance of the institution or service provider is likely. Risk management processes may not effectively identify risks, and may not be appropriate for the size, complexity, or risk profile of the entity. Strategic plans are vaguely defined and may not provide adequate direction for IT initiatives. As a result, management often has difficulty responding to changes in business, market, and technological needs of the entity. Self-assessment practices are weak and are generally reactive to audit and regulatory exceptions. Repeat concerns may exist indicating that management may lack the ability or willingness to resolve concerns. The financial condition of the service provider may be weak and/or negative trends may be evident. While financial or operational failure is unlikely, increased supervision is necessary. Formal or informal supervisory action may be necessary to secure corrective action.

Composite 4

Financial institutions and service providers rated ''4'' operate in an unsafe and unsound environment that may impair the future viability of the entity.

Operating weaknesses are indicative of serious managerial deficiencies. Risk management processes inadequately identify and monitor risk, and practices are not appropriate given the size, complexity, and risk profile of the entity. Strategic plans are poorly defined and not coordinated or communicated throughout the organization. As a result, management and the board are not committed to, or may be incapable of insuring that technological needs are met. Management does not perform self-assessments and demonstrates an inability or willingness to correct audit and regulatory concerns. The financial condition of the service provider is severely impaired and/or deteriorating. Failure of the financial institution or service provider may be likely unless IT problems are remedied. Close supervisory attention is necessary and, in most cases, formal enforcement action is warranted.

Composite 5

Financial institutions and service providers with a composite rating ''5'' exhibit critically deficient operating performance and are in need of immediate remedial action. Operational problems and serious weaknesses may be apparent throughout the organization. Risk management processes are severely deficient and provide management little or no perception of risk relative to the size, complexity, and risk profile of the entity. Strategic plans do not exist or are ineffective, and management and the board provide little or no direction for IT initiatives. As a result, management is unaware of, or inattentive to technological needs of the entity. Management is incapable of identifying and correcting audit and regulatory concerns. The financial condition of the service provider is poor and failure is highly probable due to poor operating performance or financial instability. Formal enforcement action and ongoing supervision is required.

Component Ratings [2]

Audit

Financial institutions and service providers are expected to provide independent assessments of their exposure to risks and the quality of

[1] The descriptive examples in the numeric composite rating definitions are intended to provide guidance to examiners as they evaluate the overall condition of Information Technology. Examiners must use professional judgement when making this assessment and assigning the numeric rating.

[2] The descriptive examples in the numeric component rating definitions are intended to provide guidance to examiners as they evaluate the individual components. Examiners must use professional judgement when assessing a component area and assigning a numeric rating value as it is likely that examiners will encounter conditions that correspond to descriptive examples in two or more numeric rating value definitions.

internal controls associated with the implementation and use of information technology.[3] Audit practices should address the IT risk exposures throughout the institution and its service provider(s) in the areas of user and data center operations, client/server architecture, local and wide area networks, telecommunications, information security, electronic data interchange, systems development, and contingency planning. This rating should reflect the adequacy of the organizations overall IT audit program, including the internal and external auditor's abilities to detect and report significant risks to management and the board of directors on a timely basis. It should also reflect the internal and external auditor's capability to promote a safe, sound, and effective operation.

The performance of audit is rated based upon an assessment of:

- The level of independence maintained by audit and the quality of the oversight and support provided by the board of directors and management.
- The adequacy of audit's risk analysis methodology used to prioritize the allocation of audit resources and formulate the audit schedule.
- The scope, frequency, accuracy, and timeliness of internal and external audit reports.
- The extent of audit participation in application development, acquisition, and testing, to ensure the effectiveness of internal controls and audit trails.
- The adequacy of the overall audit plan in providing appropriate coverage of IT risks.
- The auditors adherence to codes of ethics and professional audit standards.
- The qualifications of the auditor, staff succession, and continued development through training and continuing education.
- The existence of timely and formal follow-up and reporting on management's resolution of identified problems or weaknesses.
- The quality and effectiveness of internal and external audit activity as it relates to IT controls.

Ratings

1. A rating of ''1'' indicates strong audit performance. Audit independently identifies and reports weaknesses and risks to the board of directors or its audit committee in a thorough and timely manner. Outstanding audit issues are monitored until resolved. Audit risk analysis ensures that audit plans address all significant IT operations, procurement, and development activities with appropriate scope and frequency. Audit work is performed in accordance with professional auditing standards and report content is timely, consistent, accurate, and complete. Because audit is strong, examiners may place substantial reliance on audit results.

2. A rating of ''2'' indicates satisfactory audit performance. Audit independently identifies and reports weaknesses and risks to the board of directors or audit committee, but reports may be less timely. Significant outstanding audit issues are monitored until resolved. Audit risk analysis ensures that audit plans address all significant IT operations, procurement, and development activities; however, minor concerns may be noted with the scope or frequency. Audit work is performed in accordance with professional auditing standards; however, minor or infrequent problems may arise with the timeliness, completeness and accuracy of reports. Because audit is satisfactory, examiners may rely on audit results but because minor concerns exist, examiners may need to expand verification procedures in certain situations.

3. A rating of ''3'' indicates less than satisfactory audit performance. Audit identifies and reports weaknesses; however, independence may be compromised and reports presented to the board or audit committee may be less than satisfactory in content and timeliness. Outstanding audit issues may not be adequately monitored. Audit risk analysis is less than satisfactory. As a result, the audit plan may not provide sufficient audit scope or frequency for IT operations, procurement, and development activities. Audit work is generally performed in accordance with professional auditing standards; however, occasional problems may be noted with the timeliness, completeness and/or accuracy of reports. Because audit is less than satisfactory, examiners must use caution if they rely on the audit results.

4. A rating of ''4'' indicates deficient audit performance. Audit may identify weaknesses and risks but it may not independently report to the board or audit committee and report content may be inadequate. Outstanding audit issues may not be adequately monitored and resolved. Audit risk analysis is deficient and, as a result, the audit plan does not provide adequate audit scope or frequency for IT operations, procurement, and development activities. Audit work is often inconsistent with professional auditing standards and the timeliness, accuracy, and completeness of reports is unacceptable. Because audit is deficient, examiners will not rely on audit results.

5. A rating of ''5'' indicates critically deficient audit performance. If an audit function exists, it lacks sufficient independence and, as a result, does not identify and report weaknesses or risks to the board or audit committee. Outstanding audit issues are not collected and no follow up is performed to monitor their resolution. The audit risk analysis is critically deficient. As a result, the audit plan is ineffective and provides inappropriate audit scope and frequency for IT operations, procurement and development activities. Audit work is not performed in accordance with professional auditing standards and major deficiencies are noted regarding the timeliness, accuracy, and completeness of audit reports. Because audit is critically deficient examiners cannot rely on audit results.

Management

This rating reflects the abilities of the board and management as they apply to all aspects of IT 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, regulatory and legal compliance.

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 board's and management's ability as it applies to all aspects of IT operations.

For service providers of financial institutions, additional risk factors must be weighed in the management component rating such as the service provider's financial condition, continuing viability, service level performance to financial institutions, and contractual terms and plans.

The performance of management and the quality of risk management are rated based upon an assessment of:

- 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

[3] Financial institutions that outsource their data processing operations should obtain copies of internal audit reports, SAS 70 reviews, and/or regulatory examination reports of their service providers.

arise from changing business conditions.

- The ability of management to provide management 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 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.
- The ability of management to identify, measure, monitor, and control risks and to address emerging information technology needs and solutions of the organization.
- In addition to the above factors, the following are included in the assessment of management at service 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.

Ratings

1. 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.

2. 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, the implementation of corrective actions may not always be in a timely manner. Technology plans, policies and 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 which 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.

3. 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 in place 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 and 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 influence decision making and performance monitoring. Outsourcing arrangements may be entered into without thorough planning. Management may provide only cursory supervision that limits their understanding of vendor contracts, performance standards, and services provided. Management and the board may not be capable of addressing existing IT problems and risks, evidenced by untimely corrective actions and outstanding IT problems.

4. 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 deficient. As a result, management may not be aware of and is unable to control risks. Management may be unwilling and/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 and/or flawed decision making. Outsourcing 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.

5. 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 and/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 and procedures, and standards are critically deficient. Because of systemic problems, IT systems do not produce management reports which 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 inappropriate vendor services.

Development and Acquisition

Development and acquisition represent 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 those. 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, and 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 management practices for acquisition, and deployment of information technology. This rating also reflects the board and management's ability to enhance and replace information technology prudently in a controlled environment.

For service providers of financial institutions, additional risks to the serviced institution, such as the quality of software releases, and the training provided to clients, must be weighed in the Development and Acquisition component rating.

The performance of systems development and acquisition and related risk management practice is rated based upon an assessment of:

- 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 systems 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 Systems 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.
- The extent of end user involvement in the system development process.

Ratings

1. 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.

2. A rating of ''2'' indicates a satisfactory systems development, acquisition, implementation, and change management performance. Management and the board frequently demonstrate their 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.

3. 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 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.

4. 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.

5. 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 have caused significant IT risks. Technology solutions do not meet the needs of the organization. Serious problems and significant risks exist which raise concern for the financial institution or service provider's ongoing viability.

Support and Delivery

Support and delivery for IT represent an organization's ability to provide technology services in a secure environment. This rating reflects not only the condition of IT operations but also factors such as reliability, security, and integrity, which may affect the quality of the information delivery system. This includes customer support and training, and the ability to manage problems and incidents, operations, system performance, capacity planning, and facility and data management. Risk management practices should promote effective, safe and sound IT operations ensuring the continuity of operations and the reliability and availability of data. The scope of this component rating includes operational risks throughout the organization and service providers.

For service providers of financial institutions, additional risk factors must be weighed in the support and delivery component rating such as the level of customer service and the management of third-party services.

The rating of IT support and delivery are based on a review and assessment of:

- The ability to provide a level of service that meets the requirements of the business.
- The adequacy of security policies, procedures, and practices in all units and at all levels of the financial institution, and service providers.
- The adequacy of data controls over preparation, input, processing, and output.
- The adequacy of corporate contingency planning and business resumption for data centers, networks, service providers and business units.
- The quality of processes or programs that monitor capacity and performance.
- The adequacy of contracts and the ability to monitor relationships with service providers.
- The quality of assistance provided to users including the ability to handle problems.
- The adequacy of operating policies, procedures, and manuals.
- The quality of physical and logical security including the privacy of data.

1. A rating of ''1'' indicates strong IT support and delivery performance. The organization provides technology services that are reliable and consistent. Service levels adhere to well-defined service level agreements and routinely meet or exceed business requirements. A comprehensive corporate contingency and business resumption plan is in place. Annual contingency plan testing and updating is performed; and, critical systems and applications are recovered within acceptable time frames. A formal written data security policy and awareness program is communicated and enforced throughout the organization. The logical and physical security for all IT platforms is closely monitored and security incidents and weaknesses are identified and quickly corrected. Relationships with third-party service providers are closely monitored. IT operations are highly reliable and risk exposure is successfully identified and controlled.

2. A rating of ''2'' indicates satisfactory IT support and delivery performance. The organization provides technology services that are generally reliable and consistent, however, minor discrepancies in service levels may occur. Service performance adheres to service agreements, and meets business requirements. A corporate contingency and business resumption plan is in place, but minor enhancements may be necessary. Annual plan testing and updating is performed; and, minor problems may occur when recovering systems or applications. A written data security policy is in place but may require improvement to ensure its adequacy. The policy is generally enforced and communicated throughout the organization, e.g. via a security awareness program. The logical and physical security for critical IT platforms is satisfactory. Systems are monitored and security incidents and weaknesses are identified and resolved within reasonable time frames. Relationships with third-party service providers are monitored. Critical IT operations are reliable and risk exposure is reasonably identified and controlled.

3. A rating of ''3'' indicates that the performance of IT support and delivery is less than satisfactory and needs improvement. The organization provides technology services that may not be reliable or consistent. As a result, service levels periodically do not adhere to service level agreements or meet business requirements. A corporate contingency and business resumption plan is in place but may not be considered comprehensive. The plan is periodically tested; however, the recovery of critical systems and applications is frequently unsuccessful. A data security policy exists; however, it may not be strictly enforced or communicated throughout the organization. The logical and physical security for critical IT platforms is less than satisfactory. Systems are monitored; however, security incidents and weaknesses may not be resolved in a timely manner. Relationships with third-party service providers may not be adequately monitored. IT operations are not acceptable and unwarranted risk exposures exist. If not corrected, weaknesses could cause performance degradation or disruption to operations.

4. A rating of ''4'' indicates deficient IT support and delivery performance. The organization provides technology services that are unreliable and inconsistent. Service level agreements are poorly defined and service performance usually fails to meet business requirements. A corporate contingency and business resumption plan may exist, but its content is critically deficient. If testing is performed, management is typically unable to recover critical systems and applications. A data security policy may not exist. As a result, serious supervisory concerns over security and the integrity of data exist. The logical and physical security for critical IT platforms is deficient. Systems may be monitored, but security incidents and weaknesses are not successfully identified or resolved. Relationships with third-party service providers are not monitored. IT operations are not reliable and significant risk exposure exists. Degradation in performance is evident and frequent disruption in operations has occurred.

5. A rating of ''5'' indicates critically deficient IT support and delivery performance. The organization provides technology services that are not reliable or consistent. Service level agreements do not exist and service performance does not meet business requirements. A corporate contingency and business resumption plan does not exist. Testing is not performed and management has not demonstrated the ability to recover critical systems and applications. A data security policy does not exist and a serious threat to the organization's security, and data integrity exists. The logical and physical security for critical IT platforms is inadequate and management does not monitor systems for security incidents and weaknesses. Relationships with third-party service providers are not monitored and the viability of a service provider may be in jeopardy. IT operations are severely deficient and the seriousness of weaknesses could cause failure of the financial institution or service provider, if not addressed.

[End of Proposed Text of Uniform Rating System for Information Technology]

Dated: June 3, 1998.

Keith Todd,

Acting Executive Secretary, Federal Financial Institutions Examination Council.

[FR Doc. 98–15231 Filed 6–8–98; 8:45 am]

BILLING CODE 6210–01–P 6720–01–P 4810–33–P 6714–01–P

FEDERAL MARITIME COMMISSION

Notice of Agreement(s) Filed

The Commission hereby gives notice of the filing of the following agreement(s) under the Shipping Act of 1984.

Interested parties can review or obtain copies of agreements at the Washington, DC offices of the Commission, 800 North Capitol Street, NW., Room 962. Interested parties may submit comments on an agreement to the Secretary, Federal Maritime Commission, Washington, DC 20573, within 10 days of the date this notice appears in the **Federal Register**.

Agreement No.: 217–011624

Title: Lykes/TMM Space Charter Agreement

Parties:

Transportacion Maritima Mexicana S.A. de C.V. (''TMM'')

Lykes Lines Limited, LLC (''Lykes'')

Synopsis: The proposed Agreement authorizes Lykes to charter space to TMM and for the parties to enter into related cooperative arrangements in the trade between U.S. Gulf and South Atlantic Coast ports and ports in North Europe and Mexico

Dated: June 4, 1998.

By Order of the Federal Maritime Commission.

Ronald D. Murphy,

Assistant Secretary.

[FR Doc. 98–15334 Filed 6–8–98; 8:45 am]

BILLING CODE 6730–01–M

FEDERAL RESERVE SYSTEM

Agency Information Collection Activities: Proposed Collection; Comment Request

AGENCY: Board of Governors of the Federal Reserve System

SUMMARY: *Background.*

On June 15, 1984, the Office of Management and Budget (OMB) delegated to the Board of Governors of the Federal Reserve System (Board) its approval authority under the Paperwork Reduction Act, as per 5 CFR 1320.16, to approve of and assign OMB control numbers to collection of information requests and requirements conducted or sponsored by the Board under conditions set forth in 5 CFR 1320 Appendix A.1. Board-approved collections of information are incorporated into the official OMB inventory of currently approved collections of information. Copies of the OMB 83-Is and supporting statements and approved collection of information instruments are placed into OMB's public docket files. The Federal Reserve may not conduct or sponsor, and the respondent is not required to respond to, an information collection that has been extended, revised, or implemented on or after October 1, 1995, unless it displays a currently valid OMB control number.

Request for comment on information collection proposals.

The following information collections, which are being handled under this delegated authority, have received initial Board approval and are hereby published for comment. At the end of the comment period, the proposed information collections, along with an analysis of comments and recommendations received, will be submitted to the Board for final approval under OMB delegated authority. Comments are invited on the following:

a. Whether the proposed collections of information are necessary for the proper performance of the Federal Reserve's functions; including whether the information has practical utility;

b. The accuracy of the Federal Reserve's estimate of the burden of the proposed information collections, including the validity of the methodology and assumptions used;

c. Ways to enhance the quality, utility, and clarity of the information to be collected; and

d. Ways to minimize the burden of information collection on respondents, including through the use of automated collection techniques or other forms of information technology.

DATES: Comments must be submitted on or before August 10, 1998.

ADDRESSES: Comments, which should refer to the OMB control number or agency form number, should be addressed to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, 20th and C Streets, N.W., Washington, DC 20551, or delivered to the Board's mail room between 8:45 a.m. and 5:15 p.m., and to the security control room outside of those hours. Both the mail room and the security control room are accessible from the courtyard entrance on 20th Street between Constitution Avenue and C Street, N.W. Comments received may be inspected in room M-P-500 between 9:00 a.m. and 5:00 p.m., except as provided in section 261.14 of the Board's Rules Regarding Availability of Information, 12 CFR 261.14(a).

A copy of the comments may also be submitted to the OMB desk officer for the Board: Alexander T. Hunt, Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Room 3208, Washington, DC 20503.

FOR FURTHER INFORMATION CONTACT: A copy of the proposed form and instructions, the Paperwork Reduction Act Submission (OMB 83-I), supporting statement, and other documents that will be placed into OMB's public docket files once approved may be requested from the agency clearance officer, whose name appears below.

Mary M. McLaughlin, Chief, Financial Reports Section (202-452-3829), Division of Research and Statistics, Board of Governors of the Federal Reserve System, Washington, DC 20551. Telecommunications Device for the Deaf (TDD) users may contact Diane Jenkins (202-452-3544), Board of Governors of the Federal Reserve System, Washington, DC 20551.

Proposal to approve under OMB delegated authority the extension for three years, with revision, of the following report:

1. Report title: Bank Holding Company Report of Changes in Investments and Activities

Agency form number: FR Y-6A

OMB control number: 7100-0124

Frequency: on occasion

Reporters: bank holding companies

Annual reporting hours: 9,233

Estimated average hours per response: 0.85

Number of respondents: 2,263

Small businesses are not affected.

General description of report: This information collection is mandatory (12 U.S.C. 1844(b) and (c)) and is not routinely given confidential treatment. However, confidential treatment for the report information can be requested, in whole or part, in accordance with the instructions to the form.

Abstract: The Bank Holding Company Report of Changes in Investments and Activities is an event-generated report filed by top-tier bank holding companies to report changes in regulated investments and activities made pursuant to the Bank Holding Company Act and Regulation Y. The report collects information relating to acquisitions, divestitures, changes in activities, and legal authority. The number of FR Y-6As submitted varies depending on the reportable activity engaged in by each bank holding company.

The Federal Reserve proposes the following revisions to the FR Y-6A: (1)