FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

Uniform Rating System for Information Technology

AGENCY: Federal Financial Institutions Examination Council.

ACTION: Notice.

SUMMARY: The Federal Financial Institutions Examination Council (FFIEC) revised the Uniform Interagency Rating System for Data Processing Operations, commonly referred to as the Information Systems (IS) rating system. The revision changed the name of the rating system to the Uniform Rating System for Information Technology (URSIT) and reflects 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 revised numerical ratings conform to the language and tone of the Uniform Financial Institution Rating System (UFIRS) rating definitions, commonly referred to as the CAMELS rating system; reformatted and clarified the component rating descriptions; emphasized the quality of risk management processes in each of the rating components; added two new component categories, ''Development and Acquisition'', and ''Support and Delivery'' as replacements for ''Systems Development and Programming'', and ''Operations''; and explicitly identified the risk types that are considered in assigning component ratings.

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 Office of the Comptroller of the Currency (OCC), members of the Federal Reserve System, or subsidiaries of registered bank holding companies or insured depository institutions are also covered by this action.

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 175, 20th and C Streets, NW, Washington, D.C. 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, D.C. 20429.

OCC: Robert J. Hemming, National Bank Examiner, (202) 874–4929, Bank Technology Unit, Office of the Comptroller of the Currency, Mail Stop 7–8, 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

On June 9, 1998, the FFIEC published a notice in the **Federal Register** (June Notice), 63 FR 31468–31475, requesting comment on proposed revisions to the Uniform Interagency Rating System for Data Processing Operations. This rating system is an internal supervisory examination 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. Under 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 activities. 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. The composite and component ratings are assigned on a ''1'' to ''5'' numerical scale. A rating of ''1'' indicates the strongest performance and management practices and the least degree of supervisory concern, while a rating of ''5'' indicates the weakest performance and management practices and, therefore, the highest degree of supervisory concern.

The IS rating system has proven to be an effective means for the federal and state supervisory agencies to assist examiners in determining 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. As a result the FFIEC is renaming the rating system to the Uniform Rating System for Information Technology (URSIT) and making certain enhancements to the rating system, while retaining its basic framework. The URSIT enhancements:

- ☐ Realign the URSIT rating definitions to bring them in line with UFIRS.
- ☐ Replace the current ''Systems Development and Programming'' and ''Operations'' components with two new component categories, ''Development and Acquisition'' and ''Support and Delivery''.
- ☐ Reinforce the importance of risk management processes with language in each of the rating components emphasizing the consideration of processes to identify, measure, monitor, and control risks.

Comments Received and Changes Made

The FFIEC received eight comments regarding the proposed revisions to the URSIT. Three of the comments were from banks and credit unions, two from third party service providers, two from financial institution trade associations, and one from a technology vendor.

Examiners field-tested the revised rating system during bank and thrift information system examinations conducted between June and August 1998. The examiners provided comments regarding the revised rating system. Examiner responses were generally favorable, and no significant problems or unanticipated rating differences were encountered between the former and updated rating system.

The FFIEC carefully considered each comment and examiner response and made certain changes. The following discussion describes the comments received (both through public comment and agency field-testing) and changes made to the URSIT in response to those comments. The updated URSIT is included at the end of this Notice.

June Notice Specific Questions

In addition to requesting general comments regarding the proposed system, the FFIEC invited comments on six specific questions:

1. Does the proposal capture the essential risk areas of information technology?

The majority of the responses to this question were positive, and no changes were made. One commenter expressed concerns that the significance of contingency planning in maintaining

mission-critical applications in the event of a computer system failure was not adequately addressed. This concern is addressed later in this Notice under Contingency Planning.

2. Does the proposal adequately address distributed processing environments, as well as centralized processing environments?

The majority of the responses to this question were positive. Two commenters expressed concerns that the proposal did not adequately address distributed processing environments. One commenter recommended that specific language be used to emphasize network security issues, electronic commerce, and Internet controls. The FFIEC has added language to the Support and Delivery component to explicitly include electronic commerce and the Internet. One commenter expressed concerns that the proposal does not address the complexities and risks of contingency planning and data recovery in a distributed processing environment. This concern is addressed later in this Notice under Data Processing Service Providers and Contingency Planning.

3. Does the proposal adequately address risks to financial institutions that process their data in-house as well as to data processing service providers?

The majority of responses to this question were positive. Three commenters noted concerns regarding the proposal's adequacy to address risks to data processing service providers. This concern is addressed later in this Notice under 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?

The majority of responses to this question were positive. Two commenters recommended revisions in the language of the proposal to make it more consistent with UFIRS. The FFIEC made additional changes in the language of the URSIT to make it more consistent with UFIRS.

5. Are there any components which should be added to or deleted from the proposal?

The majority of the responses to this question were negative. One commenter recommended that a fifth component entitled ''Contingency Planning'' be added to the URSIT. This recommendation is addressed later in this Notice under Contingency Planning.

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?

The majority of the responses to this question were positive, and no changes were made. One commenter suggested that the integration of the examination functions deserve more study. This commenter expressed a concern that the convergence of information technology applications to the operation of the payments system is likely to result in considerable duplication in the examination process and an inconsistent evaluation of risk management procedures for information technology activities and payments system risk. The FFIEC is working toward the integration of the safety and soundness and information technology examination functions. This concern is addressed later in this notice under Risk Management.

Data Processing Service Providers

Two commenters expressed concerns that the URSIT provides little guidance regarding the differentiation of data processing service providers whose operations vary by size and complexity. The FFIEC designed the rating system so that examiners could adapt its concepts to entities of various size and complexity. Examination strategies and objectives are written based on the guidelines in the FFIEC Information Systems Examination Handbook [1] (IS Handbook). Specifically for data processing service providers this guidance is contained in Chapter 22 of the IS Handbook and generally for all entities in Chapters 2 through 5. The FFIEC oversees the application of the URSIT through its Information Systems Subcommittee. Future editions of the FFIEC IS Handbook will be reviewed and edited to ensure it continues to provide appropriate guidance for the application of the URSIT to all data processing service providers.

One commenter expressed a concern that the URSIT does not adequately address what banks, who use data processing service providers, should do in situations where their control is limited. Guidance for banks who receive data processing services is available from Chapter 22 of the FFIEC IS Handbook. This chapter specifically addresses control and administration issues in contracting with and monitoring service providers. The FFIEC designed the URSIT so that examiners could apply the concepts of the rating system to institutions who perform their data processing in-house as well as to those institutions who outsource this function to a third-party. The flexibility of the URSIT allows an examiner to include, within the scope of examination, the appropriate requirements and exclude those requirements that do not apply.

Risk Management

The revised rating system reflects an increased emphasis on risk management processes. One commenter expressed concern about whether the increased emphasis on risk management in the URSIT will be implemented and applied in a manner that is consistent with risk management principles articulated in other bank supervision initiatives, particularly those dealing with payments system risk. The FFIEC is working toward the integration of the safety and soundness and information technology examination functions. The future implementation of an integrated examination process by the FFIEC will need to address the consistent application of risk management principles and oversight of information technology activities and other operational areas. Accordingly, the FFIEC will review the URSIT periodically to ensure its compatibility with the evolving examination process. In the interim, the assessment of information technology risk management is guided by Chapter 2 of the FFIEC IS Handbook and other policy statements deemed appropriate.

Contingency Planning

One commenter suggested that the URSIT should formally address contingency planning guidelines under a separate rating to assess an institution's ability to quickly recover from a major disruption without risking a loss of its data. The commenter suggested the URSIT should include ratings that reflect a more comprehensive assessment of an institution's contingency plan and that they should define the time needed for an institution to resume core applications.

The FFIEC agrees that contingency planning and business resumption is important to the viability of any financial institution. To supervise and assess these activities, the FFIEC's revised interagency policy on Corporate Business Resumption and Contingency Planning (SP–5) provides general policies for financial institutions. This policy establishes goals and accountability for contingency planning and defines a financial institution's responsibilities regarding contingency

[1] Federal Financial Institutions Examination Council, Information Systems Examination Handbook, 1996.

planning if they have outsourced information processing. The FFIEC IS Handbook, which provides general control and verification procedures for examiners, supplements this policy. The IS Handbook also provides reference information that supports the contingency planning procedures. The IS Handbook guidance is considered sufficient to assess the adequacy of the financial institution's contingency planning efforts.

The rating system includes contingency planning as part of the assessment of the support and delivery component. The FFIEC considered stratification of the rating system components based on functional controls, e.g., contingency planning or security, and chose to use the model created by the Information Systems Audit and Control Foundation, COBIT.[2] The FFIEC concluded that further breakdown was not necessary or beneficial to the examiners or financial institutions.

Implementation Date

The FFIEC recommends that the Federal supervisory agencies implement the updated URSIT no later than April 1, 1999.

Uniform Rating System for Information Technology

Introduction

The quality, reliability, and integrity of a financial institution or service provider's information technology (IT) affects all aspects of its performance. An assessment of the technology risk management framework is necessary whether or not the institution 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 or performance requires special supervisory attention. The rating system includes component and composite rating descriptions and the explicit identification of risks and assessment factors that examiners consider in assigning component ratings. Additionally, information technology can affect the risks associated with financial institutions. The effect on credit, operational, market, reputation, strategic, liquidity, interest rate, and compliance risks should be considered for each IT rating component.

The primary purpose of the rating system is to identify those entities whose condition or performance of information technology functions 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 risk management performance, 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 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 FFIEC recognizes that management practices, particularly as they relate to risk management, vary considerably among financial institutions and service bureaus depending on their size and sophistication, the nature and complexity of their business activities and their risk profile. Accordingly, the FFIEC also recognizes that for less complex information systems environments, detailed or highly formalized systems and controls are not required to receive the higher composite and component ratings.

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[3]

Composite 1

Financial institutions and service providers rated composite ''1'' exhibit strong performance in every respect and generally have components rated 1 or 2. 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 audit and regulatory concerns. The

[2] Information Systems Audit and Control Foundation, COBIT—Governance, Control and Audit for Information and Related Technology, Second Edition.

[3] 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.

financial condition of the service provider is strong and overall performance shows no cause for supervisory concern.

Composite 2

Financial institutions and service providers rated composite ''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 informal and 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 composite ''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 ensuring that technological needs are met. Management does not perform self-assessments and demonstrates an inability or unwillingness 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 rated composite ''5'' exhibit critically deficient operating performance and are in need of immediate remedial action. Operational problems and serious weaknesses may exist 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 unwilling or incapable of 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. Ongoing supervisory attention is necessary.

Component Ratings [4]

Audit

Financial institutions and service providers are expected to provide independent assessments of their exposure to risks and the quality of internal controls associated with the acquisition, implementation and use of information technology.[5] 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 organization's 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 factors such as:

☐ 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 to 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 auditor's adherence to codes of ethics and professional audit standards.

☐ The qualifications of the auditor, staff succession, and continued development through training.

☐ 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.

---

[4] 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.

[5] 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.

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. 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, constructive, 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. 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 and risks; 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. 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. Risk analysis is deficient. 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 cannot 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 tracked and no follow-up is performed to monitor their resolution. 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 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, 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 board's and management's ability 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.

☐ 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 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.

☐ The propriety of contractual terms and plans.

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, corrective actions may not always be implemented 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 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 affect 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 for 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 risk 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. 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.

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 ineffective vendor services. The financial condition of the service provider presents an imminent threat to its viability.

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, 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 boards 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 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.

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.

☐ The adequacy of training provided to clients.

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 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.

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 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.

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 mange 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, impelementation, 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 which raise concern for the financial institution's or service providers's ongoing viability.

Support and Delivery

This rating reflects an organization's ability to provide technology services in a secure environment. It 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. The factors include 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 that ensure 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.

The rating of IT support and delivery is based on a review and assessment of requirements such as:

☐ 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 controls and the ability to monitor controls at 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.

☐ The adequacy of firewall architectures and the security of connections with public networks.

In addition to the above, factors such as the following are included in the

assessment of support and delivery at service providers:

☐ The adequacy of customer service provided to clients.

☐ The ability of the entity to provide and maintain service level performance that meets the requirements of the client.

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 contingency 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. Contingency 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.

Dated: January 13, 1999.

Keith J. Todd,

Executive Secretary, Federal Financial Institutions Examination Council.

[FR Doc. 99–1175 Filed 1–19–99; 8:45 am]

BILLING CODE 6210–01–P, 6720–01–P, 6714–01–P and 4810–33–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.: 202–010689–080.

Title: Transpacific Westbound Rate Agreement.

Parties: Kawasaki Kisen Kaisha, Ltd., A.P. Moller-Maersk Line, Mitsui O.S.K. Lines, Ltd., Nippon Yusen Kaisha, Ltd., Orient Overseas Container Line, Inc., Sea-Land Service, Inc.

Synopsis: The proposed amendment provides that members to individual service contracts subject to the Agreement, which are filed through and by the Agreement staff, may authorize the Agreement Manager to execute such contracts on their behalf.

Dated: January 13, 1999.

By order of the Federal Maritime Commission.

Bryant L. VanBrakle,

Secretary.

[FR Doc. 99–1176 Filed 1–19–99; 8:45 am]

BILLING CODE 6730–01–M

FEDERAL MARITIME COMMISSION

Notice of Agreement(s) Filed

The Commission hereby gives notice of the filing of the following