IT Examinations – Back to the Future with URSIT

1.) Introduction and Overview

On March 6, 2019, the FFIEC published a policy statement rescinding the 1993 Policy Statement on the Uniform Core Report of Examination (ROE) and issued a standard principal-based approach for all examination reports issued by the FRB, FDIC, OCC, NCUA, CFPB, and state authorities. While advances in technology were stated as a reason for the rescission, no specific guidance was issued by the FFIEC regarding IT evaluations in the ROE going forward.

Relying on frequent formal and informal communication with the respective regulatory entities, NETBankAudit has ascertained that the ROE's have revitalized the somewhat dormant URSIT format established on January 20, 1999 (Federal Register Volume 64, Number 12). This analysis also included a canvassing of clients (over 750 clients served in 37 states - regulated by the FRB, FDIC, OCC, or NCUA).

URSIT is an acronym for the "Uniform Rating System for Information Technology" and was established in 1978 and later revised in 1999. The major 1999 revisions included:

- Additional language to conform the URSIT to the Uniform Financial Institution Rating System (UFIRS).
- Clarification of the component ratings and a reformat of the descriptions for the ratings.
- Two new component categories -- "Development and Acquisition" and "Support and Delivery" which replace "Systems and Programming" and "Operations."
- An emphasis on the quality of risk management processes in each of the rating components.

As stated, URSIT is used to uniformly assess and rate IT-related risks of financial institutions and their technology service providers. The primary purpose of this rating system is to evaluate the examined institution's overall risk exposure and risk management performance and determine the degree of supervisory attention necessary to ensure that weaknesses are addressed, and risks are properly managed. The assigned ratings determine the degree of supervisory attention necessary. An overall rating (High of 1 and Low of 5) as well as component ratings are given for Management, Audit, Development & Acquisition, and Support & Delivery.

Key nuances to understand the evolution of URSIT are:

- In 1999 and the early 2000's, URSIT only applied to financial institutions (FIs) that operated core processing in-house (mainframe/midrange on premises). Thus, service bureau and/or outsourced core FIs received only cursory or limited IT examination reviews.
- In the early 2000's, the IT Examination Report was consolidated into the Commercial (Safety & Soundness) Examination Report. IT observations and matters requiring attention were primarily addressed in the management section under operational risk and the regulatory compliance section for GLBA 501(b) violations. The specific component (Management, Audit, Development & Acquisition, and Support & Delivery) ratings and evaluations were phased out of the ROE content over time, depending on the agency.

Currently, the regulatory agencies are using some form of URSIT evaluation and reporting, and URSIT is being applied universally to all financial institutions whether core processing is conducted in-house or outsourced. Accordingly, this series of whitepapers will address each component starting with Support & Delivery through Development & Acquisition, Audit, and Management. We will end the series with an overall conclusion, suggested strategies, and examination checklist. The purpose of this series is to educate the reader on the application and criteria of URSIT. Understanding the individual components and overall approach should lead to more effective and efficient IT examination performance.

2.) Support & Delivery

The Support & Delivery component covers "the meat and potatoes" of the financial institution's IT environment, encompassing both operations and security. Key areas of examiner focus include:

- IT Operations
  - System Design, Availability, and Capacity
  - Hardware and Software Controls
  - Change Management and Problem Management
  - Data Integrity and Input/Output Controls
  - Data Backup
  - Business Continuity and Disaster Recovery
- IT Security
  - Information Security and Cybersecurity Programs
  - Network Security
  - User Access Controls
  - Logical Access Controls
  - Physical Controls
  - Logging and Monitoring Controls
  - Incident Prevention and Response

NOTE: While Risk Assessment, Policies & Procedures, Vendor Management, etc. are typically evaluated in the Management and Development & Acquisition components, these factors may also be included in the Support & Delivery assessment as applicable to the areas listed above.

For the Operations Review, the examiner will typically start with and/or scrutinize the Disaster Recovery/Business Continuity and Incident Response Plan(s). The Information Security Risk Assessment and CAT will be the focal points of the Security Review. It is imperative that those documents are professional and in full compliance. First impressions set the correct tone for a successful examination. From there, interviews with management and the staff will proceed. These interviews will reconcile regulatory requirements and established policies with actual practices. Additionally, segregation of duties will be vetted. Proactive (*in lieu of reactive or defensive*) replies, along with well-maintained data centers and offices, will also help set the right impression. Technical evaluations tend to be limited to user access reviews. For the more technical or "hands-on" analysis, examiners generally leverage in-

house and outsourced audit and test results (e.g. vulnerability assessments and configuration audits). Be sure that missing patches and updates have been applied or formally addressed. In addition to the core and network, make certain that the wire transfer, ACH, and Internet banking functions are strictly controlled and actively monitored. Don't let web-based applications and decommissioned hardware fall off your radar.

The key to obtaining a "Satisfactory" or better Support & Delivery component rating is presenting very professionally and demonstrating sound knowledge and awareness thorough verified and documented results. To the extent that management can control the narrative without creating antagonism, all the better.

3.) Development & Acquisition

Development & Acquisition is a narrowly focused component. In the early 2000s, this component primarily covered custom coding, custom reporting, and custody of the source code for turn-key software solutions. Currently, the component has evolved to cover the following areas:

- Project Management
- Vendor Management – Due Diligence
- System Development Life Cycle (SDLC)
    - Asset Lifecycle Plan
    - Custom Coding/Custom Reporting
        - Compilers

Whether or not your institution performs custom coding and/or employs programmers sets the bar for this component. If so, the institution will be subjected to "textbook" SDLC examination procedures. Depending upon the size and complexity of the institution or project, SDLC phases may be combined, overlapped, or waived/omitted. However, the IT Steering Committee should be prepared to evaluate the following processes:

1. Project Initiation
2. Project Planning/Functional Analysis
3. Design Phase
4. Programming Development/System Setup
5. Acceptance Testing
6. Implementation
7. Post Implementation/Evaluation

After custom coding comes compilers and custom reporting on the examiner questionnaire. The common pitfalls of these areas involve chain of custody, segregation of duties, and inadequate reconcilement. Make sure that these areas are risk assessed, documented (mapped), and validated on a regular basis.

Project Management is the universal subject matter of the Development & Acquisition component. You should have a Board approved Project Management Policy with verifiable supporting procedures and standards that cover the following areas:

- Risk Assessment
- Feasibility Studies and Cost/Benefit Analyses
- Vendor and Contract Reviews
- End-user Involvement
- Project Plans and Status Reports
- Test Plans and Results Documentation
- Post Implementation Reviews

Most of the examination issues regarding Project Management tend to be administrative in nature. It is important to have a formal and thorough policy. From there, focus on the risk assessment. Make sure likelihood and impact are addressed along with operational and security threats and risks. The scoring system should be clear, meaningful, and include inherent and residual risks. Vendor Reviews, Project Plans with regular status reporting, and Test Result Documentation will be key in demonstrating compliance with FFIEC guidance.

Vendor Management is included in several URSIT components. In Development & Acquisition, Vendor Management Due Diligence is the focus. Accordingly, one should consider and document the following factors regarding the selection of your service providers (as applicable):

- Existence and corporate history;
- Qualifications, backgrounds, and reputations of company principals, including criminal background checks where appropriate;
- Other companies using similar services from the provider that may be contacted for reference;
- Financial status, including reviews of audited financial statements;
- Strategy and reputation;
- Service delivery capability, status, and effectiveness;
- Technology and systems architecture;
- Internal controls environment, security history, and audit coverage;
- Legal and regulatory compliance including any complaints, litigation, or regulatory actions;
- Reliance on and success in dealing with third-party service providers;
- Insurance coverage; and
- Ability to meet disaster recovery and business continuity requirements.

Asset Lifecycle Planning is also an area of consideration. Hardware and Software Inventories should be accurate and kept up to date. Lifecycle and Disposal Plans should be in place. If the need for outdated hardware and software persists, this need should be risk assessed and documented, particularly with regards to Patch Management.

The key to obtaining a “Satisfactory” or better Development & Acquisition component rating is documentation, documentation, documentation. Having a thorough and professional Project Management Policy that is Board approved with a sound risk assessment(s) will go a long way with determining a successful examination outcome. Additionally, make sure that your IT Steering Committee minutes include Project Management and Tracking as a regular discussion topic. Having detailed inventories and diagrams adds further validation.

4.) IT Audit

The Audit component is also a narrowly focused component; however, the ability or inability to obtain an adequate IT Audit directly affects the IT Management component rating. Thus, the IT Audit is a major factor in determining overall URSIT performance. It is also important to note that examinations are not "hands-on" or go as deep as audits. Accordingly, the examination team relies heavily on audit evaluations and findings. The IT Audit Component considers the following aspects:

- Level of Independence
- Adequacy of Risk Analysis
- Scope, Frequency, Accuracy, & Timeliness
- Audit Validation
- Audit Plan & Schedule
- Adherence to Code of Ethics
- Auditor Qualifications
- Issue Tracking & Follow-up
- Audit Activity & Internal Control Alignment

Independence should be clearly established in the Audit Charter and by the Audit Committee. IT management controlling the contracting process for outsourced IT Audits is a commonly noted examination exception regarding independence. All proposals, contracts, risk assessments, reports, etc. should be reviewed and approved by the Audit Committee and the designated Internal Audit/Risk Management function.

The IT Audit Risk Assessment is a critical document. The risk assessment must address both the likelihood and impact of threats and risks associated with operational malfunctions and/or security incidents. The risk assessment should cover all IT-related systems and processes and their respective vulnerabilities and controls. A formal scoring system should be established. Scores should be clear, meaningful, and include inherent and residual risks. While overlap with other IT-related risk assessments will occur, the purpose of the IT Audit Risk Assessment is to determine the allocation of audit resources (i.e. hours). Thus, a one-for-one alignment with other risk assessments (e.g., high-risk systems with low-risk errors/issues) may not occur. Once the IT Audit Risk Assessment has been reviewed, vetted, and approved, the audit plan and schedule should be established based on the risk analysis. The risk assessment should be updated after the audit, when a significant change or event occurs, and before the audit. The scope and frequency of the IT Audit should be based on the IT Audit Risk Assessment. The FFIEC requires annual IT Audit coverage. More frequent reviews may be necessary given the high risks associated with respective IT systems and processes (e.g., FFIEC Cybersecurity Baseline requires quarterly firewall audits). Fundamentally, the risk assessment must comply with the Board's risk appetite and FFIEC guidance.

The IT audit report should be thorough, accurate, and supported by detailed work papers. Generally speaking, the final IT report and associated work papers should be issued within 30 days of the onsite exit meeting. All reports and workpapers should be retained by the financial institution. If the vendor stores the reports and work papers for the client, all documentation should be supplied promptly to the financial institution upon request and for examination purposes. With regards to the work papers, the

IT Audit should document all audits steps in a formal work program. These steps should be risk-based and provide verification that the audit objective has been met or not met.

All IT Auditors should be certified and adhere to a code of ethics. We recommend the COBIT methodology and the CISA certification. COBIT (Control Objectives for Information and Related Technologies) is a framework created by ISACA (Information Systems Audit and Control Association). ISACA is an independent, nonprofit, global association that engages in the development, adoption and use of globally accepted information system (IS) knowledge and practices. The CISA (Certified Information Systems Auditor) designation is sponsored by ISACA. It requires five years of experience and practical application along with educational and examination requirements. Once certified, ongoing education and association is required. We recommend the COBIT methodology and the CISA certification because it is endorsed by the FFIEC and all examiners across the agencies are familiar with the methodology and seek to obtain the certification. In addition to auditor certification, NETBankAudit also stresses senior level competence and experience. A key part of an effective and efficient IT audit is practical knowledge sharing and value-add. The IT audit should add value to your organization in addition to attesting to controls. Accordingly, the auditor should have a strong background and/or experience in actual operations, networking, and regulatory affairs. Former regulators, network administrators, CIOs, COOs, etc., are generally more effective and efficient auditors given their various experiences and perspectives.

IT Audit follow-up and issue tracking is a commonly reported examination issue. All audit issues should be documented, tracked, and resolved promptly based on risk and priority. Risk acceptance of reported issues should be done judiciously, and such risk acceptances should be thoroughly documented by the Audit Committee and Risk Management function. Repeat issues are considered significant examination deficiencies and often used to justify unsatisfactory examination ratings.

Overall, the IT audit should align with the IT examination. While the two are different in their scope and objectives, the overall evaluation and findings should be consistent with one another. Further, the goal of a successful IT Audit from a regulatory perspective is to supplement the IT examination process. In essence, the IT Audit should lay the groundwork for the IT examination team and make the IT exam less intrusive. At NETBankAudit, we spend considerable time, effort, and resources ensuring this efficiency for all of our clients. It is a vital component our value-add philosophy that all financial institutions should expect and require.

5.) IT Management

The Management component is broad by nature and includes IT Governance. Specifically, the Management Component considers the following aspects:

- Board Governance
- Organizational Structure
- IT Strategic Planning & IT Budget
- IT Reporting & Monitoring
- Policies, Procedures, & Standards

- Risk Assessment & Monitoring
- Corrective Action
- Regulatory Compliance
- Vendor Management
- Training and Awareness

The keys and/or areas of focus to the above are listed below:

- **Board Governance:** Formally chartered IT Steering Committee, active discussion documented in Board minutes of IT-related issues including annual review and approval of all IT-related plans, programs, policies, and risk assessments.
- **Organization Structure:** current and accurate organizational charts, Independent Information Security Officer appointed, written job descriptions, segregation of duty controls, management succession planning, qualified backup personnel.
- **IT Strategic Planning & IT Budget:** short-term and long-term, aligns with corporate strategic plan and budget, Board approved.
- **IT Reporting & Monitoring:** Project Management, Audit and Examination, BCP test results, Daily Operational and Security Metrics including Patch Management, Capacity Planning. IT Reporting and Monitoring should be documented in Board minutes under the IT Steering Committee minutes.
- **Policies, Procedures, & Standards:** Policy establishes governance, procedures provide employee guidance, and standards provide compliance parameters. Key programs that receive most examination attention are Information Security/Cybersecurity, Business Continuity, Incident Response, Vendor Management, Project Management, and Change Management. Make sure these documents are reviewed and approved by the Board on an annual (or more frequent) basis and follow FFIEC guidance. Accurate and detailed network diagrams.
- **Risk Assessment and Monitoring:** all risk assessments should align with the Board's risk appetite and address applicable threats and vulnerabilities in the context of likelihood (%) and impact ($). The general formula for risk assessments is inherent risks less controls equals residual risks. A substantive scoring system is strongly recommended. Key risk assessments that receive examiner scrutiny are Information Security, Cybersecurity (CAT), Business Continuity/BIA, Internet Banking, Vendor Management, Project Management, ACH/Wire Transfer, Remote Deposit Capture, Identity Theft, and Social Media.
- **Corrective Action:** Formal tracking, reporting, and prompt (complies with target date) resolution of audit and examination issues. Incident Response procedures and reporting requirements are followed, documented, and include resolution and forensic measures.
- **Regulatory Compliance:** GLBA 501(b) along with newer cybersecurity guidance, Identity Theft/Red Flags, and FFIEC Guidance (IT Booklets).
- **Vendor Management:** Due Diligence and Ongoing Monitoring of vendors should encompass and include all respective FFIEC guidance checklist items. Risk Assessment: make sure High, Medium, and Low Risk Vendor Files comply with internal policy and FFIEC guidance.
- **Training and Awareness:** Information Security Training with social engineering testing. Business Continuity Training. Continual educational program for IT staff. All training should be regular, have appropriate participation levels, and be well documented.

To obtain a satisfactory or better Management URSIT rating, management and the Board need to demonstrate effective risk management and oversight practices as well as the ability to successfully address existing problems. Substantiation starts with risk assessments, policy frameworks, and dynamic Board and IT Steering Committee minutes. While these documents need to comply fully to the FFIEC guidance, they also need to be tailored specifically to the financial institution's IT environment. Resolution of all outstanding audit and exam issues is imperative. During examination interviews and interaction, the respective officer or manager should convey a consistent and coherent message with regards to the program in question or under examination. We do not recommend providing program documentation to an examiner without accompanying verbal presentation and clarification. Polite, professional, and proactive communication is always the key to any successful examination.

As evidenced above, IT Management is a broad category. The examiner most likely will not cover all of the above in detail. However, the more details and documentation that you have prior to the examination, the greater success you will have.

6.) Summary Conclusion & Checklist

Once you have garnered an overall understanding of URSIT and each individual component, we recommend that you develop your examination strategy, accordingly. The regulators will appreciate your grasp of the evaluation structure, and this approach should make the examination process easier.

Start with the IT Audit component. Most financial institutions outsource at least a portion of the IT Audit function. Make sure that the selected firm has a very good understanding of URSIT, as well as FFIEC (FDIC, FRB, OCC, NCUA, and state) guidelines. Ideally, the examiner should be able to leverage your IT Audit and reduce exam processes to clarification and inquiry.

Once you are comfortable with your IT Audit performance, take inventory of the Support & Delivery requirements and expectations. As previously explained, the Support & Delivery component includes the bulk of the technical and operational evaluation. The Development & Acquisition component primarily focuses on project management and vendor management unless in-house programming is conducted.

Lastly, we recommend concluding with the IT Management component to tie everything together. Leadership should review and ensure an appropriate level of performance for the other three components, as well as the fulfillment of Management and Board oversight requirements. A checklist by component is provided below for additional support:

- ✓ **IT Audit**
  - IT Audit Risk Assessment
    - Comprehensive, Sound Methodology, Audit Committee Approved
  - Outsourced IT Audit Firm

        - Complies with FFIEC Vendor Management requirements
        - Audit Committee vetted and approved
            - *Exam Gotcha: IT Manager signs IT Audit contract*
    - IT Audit and Exam Issues tracked and resolved promptly
        - *Exam Gotcha: Repeat issues*
    - IT Audit report *and work papers* promptly delivered and readily available for examination

✓ **Support & Delivery**

- Business Continuity and Disaster Recovery
    - BIA/Risk Assessment
        - *Exam Gotcha: RTOs and RPOs*
    - Data Back-up
    - Risk-based and updated testing schedules and documented results (Board reviewed)
        - *Exam Gotcha: outdated inventories and calling trees*
    - Incident Response
- Information Security
    - Information Security Risk Assessment/GLBA 501(b)
    - CAT
    - User and Logical Access
        - Add, remove, change user access
            - *Exam Gotcha: Admin access, segregation of duties*
        - Complex passwords, multi-factor
        - Workstation controls and remote access
    - Patch Management and Internal and External Vulnerability Assessments
        - Results documented, tracked, and resolved promptly
            - *Exam Gotcha: Unapplied patches for system compatibility not documented*
- Operations
    - Network Diagrams, Configurations, and Logging
        - AD Settings
    - Hardware and Software Inventories
        - Hardware Disposal
    - Capacity Planning
    - Core Settings, File Maintenance, and Parameter Changes
    - Wire Transfer, ACH, and Internet Banking internal controls
        - *Exam Gotcha: Fedline settings and Circular 6 assurance, especially for FRB regulated banks*

✓ **Development & Acquisition**

- Project Management

        - Risk Assessment
        - Tracking and Budget
            - *Exam Gotcha: Time and budget parameters not set, tracked, or addressed*
        - Board Oversight
    - Vendor Management
        - Risk Assessment
        - Due Diligence and Ongoing Monitoring
            - *Exam Gotcha: Low, Medium, or High vendor files don't comply with policy requirements*
    - System Development Life Cycle (SDLC)
        - Asset Lifecycle Plan
        - Custom Coding/Custom Reporting
            - Compilers

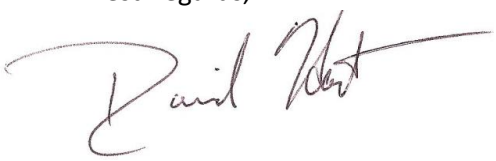
✓ **IT Management**

- Board Governance
    - IT Steering Committee Charter and Minutes
    - Should have some form of ERM system in place
    - Insurance Reviews
        - Review riders
        - *Exam Gotcha: Noncompliance with insurance requirements for ACH*
- Organizational Structure
    - Succession planning, backups, segregation of duties
- IT Strategic Planning & IT Budget
    - Align with corporate plan and budget
- IT Reporting & Monitoring
    - Incidents
    - Patch Management
    - Operational/downtimes
- Policies, Procedures, & Standards
    - Annual review and approval documented in Board minutes
- Risk Assessment & Monitoring
    - IT-related risk assessments align with corporate risk assessments and Board's risk appetite
    - Annual (more frequent as needed) review and approval
- Corrective Action
    - *Exam Gotcha: Repeat issues*
- Regulatory Compliance
    - Cybersecurity/GLBA, ID Theft/Red Flags, FFIEC IT Booklets
- Vendor Management
    - Annual review of program and policy documented in minutes
    - Due Diligence, Ongoing Monitoring, and Risk Assessment

- Training and Awareness
  - Information Security including Social Engineering testing
    - *Exam Gotcha: Employee completion percentages*
  - Ongoing technical
    - *Exam Gotcha: lack of technical expertise/certifications*

Understanding the URSIT framework in conjunction with FFIEC compliance should allow your institution to thrive during the IT examination process, given sound operational controls. While examiners differ from agency, region, and individual, the ability to respond to the regulatory reviews in the preferred manner is always a winning strategy. To the extent that this series has been helpful in explaining the approaches and nuances of URSIT, we are very pleased. If you would like to follow-up for further discussion. I am always available: 1 (800) 243-0416 Ext 527 or dhart@netbankaudit.com.

Best Regards,



David Hart
NETBankAudit President & Partner