What to Expect At Your Next Regulatory Exam

Tony DaSilva, AAP, CISA
Federal Reserve Bank of Atlanta

The opinions expressed are those of the presenters and are not those of the Federal Reserve Banks, the Federal Reserve System, or its Board of Governors.

Topics

- Electronic Banking
- Payments
- Cybercrime
- Fraud
- Cybersecurity
- FFIEC “CAT” Tool
- FFIEC Payments
- Updated InTREx

Electronic Banking
Now and the Future (No Going Back)
Electronic Banking
- Account Activity
- Internal Transfers
- Bill Pay
- RDC
- ACH
- Wire Transfer
- External Transfers
- Mobile Payments
- New Accounts
  - Deposits, Loans, (Fintech), etc.

Retail Payments
- Checks/Remote Deposit Capture
- Remotely Created Checks
- ACH
- Card Products (Debit, Credit, Stored Value)
- Merchant Acquiring
- Mobile Financial Services
FOR COMMUNITY BANKS

Also an OPPORTUNITY!
Bad guys follow the path of least resistance and most profit.

Cybercrime

Cybercrime is a well-funded, organized business with sophisticated technology. It is driven by a powerful combination of actors ranging from organized crime, nation states, and decentralized cyber gangs. They executed recent massive credit card and identity data breaches, using this data to profit from all types of fraud—card not present, account takeover, and new account creation—across all businesses across all regions.
Cybercrime – Where & Why?

- Where do cyber attacks come from?
- What is the motivation?
  - Ideology – making a political statement
  - Extortion – demand for payment to avoid website attack
  - Competition – disrupt a competitors online services
  - Fraud – used as a tool to aid in unauthorized financial gain

Threats & Consequences

- Third Party, Vendor, and Cloud
- Malware
- Ransomware
- Data Corruption
- Data Destruction
- Distributed Denial of Service (DDoS)
- Payment Account Takeovers
- Mobile Application Vulnerabilities
- Social Engineering

Trends
Ongoing Concerns

- Bank service providers as continued targets
- Overload of key service providers attempting to mitigate the effects of DDoS attacks
- Attacks moving down to banks of lower asset size with potentially less capability for managing the attacks
- DDoS attacks being used as a diversion while fraudulent wire transfers are being transmitted (and other fraudulent/malicious transactions)

Payments Cybercrime

ACH & Wire Transfers

Protect the Bank

From:

- Vendors
- Customers
- Employees
People the Weak Link

- Whether they come from email, the web, social media, or mobile apps, today’s cyber attacks have one thing in common—they all target people.
- Cyber criminals have shifted tactics. Rather than relying solely on technical exploits, today’s attacks fool humans into becoming unwitting accomplices, infecting systems, stealing credentials, and transferring funds.

Dark Web

THE TOR DARK WEB MAY BE REFERRED TO AS ONIONLAND.
TOR

Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name “The Onion Router”. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user: this includes “visits to Web sites, online posts, instant messages, and other communication forms”.

Rent-A-Hacker

Rent-A-Hacker

Technical info:

1. I'm a legit hacker.
2. I have the skills to do the job.
3. I can complete the job in a timely manner.
4. I have the necessary equipment.
5. I have ateam of experts who can help me.
6. I have access to the internet.
7. I have access to the target.
8. I have the required software.
9. I have a valid license.
10. I have a backup plan.

Important info:

1. I will not be caught.
2. I will never be traced.
3. I will never be caught.
4. I will never be traced.
5. I will never be caught.
6. I will never be traced.
7. I will never be caught.
8. I will never be traced.
9. I will never be caught.
10. I will never be traced.

Legal info:

1. This service is not available in the USA.
2. This service is available in all countries.
3. This service is only available in countries where it is legal.
4. This service is available in countries where it is legal.
5. This service is only available in countries where it is legal.
6. This service is available in countries where it is legal.
7. This service is only available in countries where it is legal.
8. This service is available in countries where it is legal.
9. This service is only available in countries where it is legal.
10. This service is available in countries where it is legal.

Contact info:

1. Email: info@rentahacker.com
2. Phone: +1 (123) 456-7890
3. Address: 123 Main Street, Anytown, USA
4. Website: www.rentahacker.com

Terms and conditions:

1. Payment is required before service.
2. Refunds are not available.
3. Service is non-refundable.
4. Service is not guaranteed.
5. Service is not insured.
6. Service is not covered by warranty.
7. Service is not covered by insurance.
8. Service is not covered by warranty.
9. Service is not covered by insurance.
10. Service is not covered by warranty.

Privacy policy:

1. Personal information is not shared.
2. No personal information is shared.
3. No personal information is shared.
4. No personal information is shared.
5. No personal information is shared.
6. No personal information is shared.
7. No personal information is shared.
8. No personal information is shared.
9. No personal information is shared.
10. No personal information is shared.
Ransomware

- Ransomware can:
  - Prevent you from accessing Windows.
  - Encrypt files so you can’t use them.
  - Stop certain apps from running (like your web browser).
  - Ransomware will demand that you pay money (a “ransom”) to get access to your PC or files. We have also seen them make you complete surveys.
  - There is no guarantee that paying the fine or doing what the ransomware tells you will give access to your PC or files again.
2016 Bangladesh Bank Heist

In February 2016, instructions to steal US$951 million from Bangladesh Bank, the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka (since recovered) and $81 million to the Philippines (about $18 million recovered). The Federal Reserve Bank of NY blocked the remaining thirty transactions, amounting to $850 million, at the request of Bangladesh Bank. It was identified later that Dridex malware was used for the attack.

Dridex

- Investigators have linked malware used by Russian and eastern European cybergangs to a string of bank heists that culminated in the record-breaking theft of US$81 million from Bangladesh’s central bank. The gangs operate in Russia and former parts of the Soviet Union, including Moldova and Kazakhstan.
- Dridex, which is used to identify the malware and the group that uses it, is spread through e-mail that infiltrate computers and harvest information like user names and passwords which are used to gain access to privileged networks.
- First spotted in 2014, Dridex is one of the most serious online threats facing consumers and businesses, said security firm Symantec. The disciplined and highly organized gang behind the malware operates in many ways like an ordinary company, following a Monday-to-Friday work week and even taking time off for Christmas.

The Next Risk: Mobile Malware

- Mobile malware has been growing in popularity:
  - Primarily targets Android platform.
  - Some early attacks were against BlackBerry.
- Malware for attacker financial gain:
  - Simple message service (SMS) to premium-rate-short code, bills victim (up to $50/message).
  - Zeus Trojan intercepts SMS messages for banking authentication systems.
- Malware for advertising delivery (search engine poisoning)
- Malware for location tracking and piracy attacks
In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time. The Assessment incorporates cybersecurity-related principles from the FFIEC Information Technology (IT) Examination Handbook and regulatory guidance, and concepts from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
Benefits to the Institution

For institutions using the Assessment, management will be able to enhance their oversight and management of the institution’s cybersecurity by doing the following:

- Identifying factors contributing to and determining the institution’s overall cyber risk.
- Assessing the institution’s cybersecurity preparedness.
- Evaluating whether the institution’s cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies.

Assessment Tool Components

Assessment’s Parts and Process

The Assessment consists of two parts:
1. Inherent Risk Profile
2. Cybersecurity Maturity

Upon completion of both parts, management can evaluate whether the institution’s inherent risk and preparedness are aligned.
Inherent Risk Profile – Risk Categories

- Technologies and Connection Types
  - Certain types of connections and technologies may pose a higher risk depending on the complexity and intensity of connections and the nature of the specific technology products or services.

- Delivery Channels
  - Onsite delivery (e.g., for products and services) may pose a higher inherent risk depending on the nature of the specific product or service offered.

- Online/Mobile Products and Technology Issues
  - Online and mobile products and technology issues often pose a higher risk depending on the nature of the specific product or service offered.

- Institutional Characteristics
  - Institutional governance and strategic plans for institution growth may contribute to inherent risk.

- External Threats
  - The volume and type of attacks (attempted or successful) impact an institution’s inherent risk exposure.

Inherent Risk Profile – Risk Levels

- Least Inherent Risk
  - An institution with a Least Inherent Risk Profile generally has very limited use of technology, for example, computers, applications, systems, and no connections. The variety of products and services are limited.

- Minimal Inherent Risk
  - An institution with a Minimal Inherent Risk Profile generally has limited complexity in terms of the technology it uses. It offers a limited variety of low-risk products and services.

- Moderate Inherent Risk
  - An institution with a Moderate Inherent Risk Profile generally uses technology that may be complex in terms of volume and sophistication.

- Significant Inherent Risk
  - An institution with a Significant Inherent Risk Profile generally uses complex technology in terms of volume and sophistication. The institution offers high-risk products and services that may include emerging technologies.

- Most Inherent Risk
  - An institution with a Most Inherent Risk Profile uses extremely complex technologies to deliver many products and services. Many of the products and services are at the highest level of risk, including those offered to other institutions. New and emerging technologies are utilized across multiple delivery channels.

Part 1: Inherent Risk Profile – Example Layout

<table>
<thead>
<tr>
<th>Category</th>
<th>Technologies and Connection Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>least</td>
<td>minimal</td>
</tr>
<tr>
<td>significant</td>
<td>extreme</td>
</tr>
<tr>
<td>moderate</td>
<td>high</td>
</tr>
<tr>
<td>most</td>
<td>complex</td>
</tr>
</tbody>
</table>

- Number of users of remote access
- Number of connections (including lines)
- Distribution of users of remote access
- Number of connections (including lines)
- Number of users of remote access
- Number of connections (including lines)
- Number of users of remote access
- Number of connections (including lines)
- Number of users of remote access
- Number of connections (including lines)
The 5 Domains

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience

Note:
The domains include assessment factors and contributing components. Within each component, declarative statements describe activities supporting the assessment factor at each maturity level. Management determines which declarative statements best fit the current practices of the institution.

Five Domains & Assessment Factors

Steps
1. Complete Part One: Inherent Risk Profile
2. Complete Part Two: Cybersecurity Maturity Assessment
3. Determine appropriate target maturity level
4. Identify any gaps between current and desired states
5. Develop implementation plans based on identified gaps
Cybersecurity Maturity

- How effective are the institution’s risk management activities and controls identified in the Assessment?
- Are there more efficient or effective means for attaining or improving the institution’s risk management and controls?
- What third parties does the institution rely on to support critical activities?
- What is the process to oversee third parties and understand their inherent risks and cybersecurity maturity?
- How does management validate the type and volume of attacks?
- Is the institution sharing threat information with peers, law enforcement, and critical third parties through information-sharing procedures?

Maturity Assessment – Maturity Levels

- **Baseline**: Baseline maturity is characterized by minimum expectations required by law and regulations or recommendation guidelines. It includes compliance with objectives, and management has reviewed and evaluated guidelines.
- **Initial**: Initial maturity is characterized by minimum compliance of documented procedures and policies, which are not always required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and distributed beyond protection of customer information to incorporate information security and privacy.
- **Intermediate**: Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk management practices and analysis are integrated into business strategies.
- **Advanced**: Advanced maturity is characterized by cybersecurity practices and analytics, which are integrated across the lines of business. Risk management processes are automated and include continuous process improvement. Accountability for risk decisions by the board is formally assigned.
- **Innovative**: Innovative maturity is characterized by sharing innovation in people, processes, and technology for the institution and the industry. This may include developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

Six-Step Cyber Threat Intelligence Process for Financial Institutions

1. Know your SPECIFIC threats and vulnerabilities.
2. **Establish outside sources of threat intelligence for your threats**.
3. Actively and continuously adjust your security controls and monitoring as appropriate to mitigate those threats.
4. Have detailed incident plans for responses to the threats, and update these plans periodically as appropriate.
5. Actively adjust your intelligence-gathering goals to address the changes in your threats and risks.
6. Additionally conduct a cyber threat analysis as part of your overall risk management governance and compliance program.
The FFIEC IT Examination Handbook (IT Handbook), "Retail Payment Systems Booklet" (booklet), provides guidance to examiners, financial institutions, and technology service providers (TSPs) on identifying and controlling risks associated with retail payment systems and related banking activities.

Financial Institutions

- Financial institutions accept, collect, and process a variety of payment instruments and participate in clearing and settlement systems. In some cases, financial institutions perform all of these tasks.
- However, independent third parties are increasingly involved in this process, introducing new risks that affect the security of financial institutions.
Electronic Payments

- Recently, a number of new payment instruments have emerged that are largely or wholly electronic.
- Electronic payment systems offer efficiency gains by allowing for rapid and convenient transmission of payment information among system participants.
- However, the emergence of a new payment mechanism can also enable the rapid propagation of fraud, money laundering, and operational disruption if data is compromised.

Emerging Technologies

- The booklet includes a new section that covers some emerging technologies in retail payment systems.
- Additional emphasis is placed on the need for improved operational, credit, legal, and compliance risk processes for retail payment products, especially for the deployment of remote and Internet-based check and ACH capture systems.

Risk Mitigation

Risk Management Methods:
- Policies, standards, and risk limits
- Underwriting, due diligence, & oversight
- Contracts and agreements
- Transaction limits and controls
- Risk monitoring and reporting
- Audit and Control Testing
Example

**Mitigate Operational Risk from Fraud by:**
- Ensuring proper due diligence including background checks
- Using fraud detection software to filter suspicious activity
- Verification/validation of transmission
- Strict adherence to credit and other related policies
- Ensuring that credit originators require pre-funding or more in-depth financial analysis and underwriting
- Ensuring appropriate limits are in place
- Establishing adequate reserves for debt originators
- Complying with NACHA and Operator rules/regulations
- Requiring and enforcing updated agreements for all originators and third-party senders
- Monitoring activity and exceptions reports on a daily basis

Examinations

- Examiners use the Tier I and Tier II Retail Payment Systems examination procedures to evaluate the policies and procedures, business processes, personnel, and internal control systems of financial institutions and technology service providers.
- Retail payment system services include checks and share draft item processing, bankcards, payment cards, ACH, EFT/POS networks, electronic bill payment, person-to-person (P2P) and account-to-account (A2A) payment systems, and many other products and services resulting from emerging advances in technology.

Examination Scope

- The examination scope should be based upon the risk profile of the financial institution or the technology service provider.
- The risk profile is determined through an assessment of the entity’s risk environment and quality of risk management practices.
Additionally

- Appendix A: Examination Procedures
- Appendix B: Glossary
- Appendix C: Schematic of Retail Payments
  Access Channels & Payments Method
- Appendix D: Laws, Regulations, and Guidance
- Appendix E: Mobile Financial Services

Mobile Financial Services

Mobile financial services (MFS) are the products and services that a financial institution provides to its customers through mobile devices. The mobile channel provides an opportunity for financial institutions of all sizes to increase customer access to financial services and decrease costs. Although the risks from traditional delivery channels for financial services continue to apply to MFS, the risk management strategies may differ.

Appendix E: MFS

The appendix addresses the following:
- MFS Technologies
- Risk Identification
- Risk Measurement
- Risk Mitigation
- Monitoring and Reporting
Updated InTREx Program

• The program has been revised to:
  – eliminate duplicative examination procedures, particularly in the cybersecurity and the information security standards work programs;
  – further risk focus examination procedures;
  – increase the flexibility for scoping supervisory activities;
  – include foreign banking organizations’ U.S. branches and agencies with less than $50 billion in U.S. assets and savings and loan holding companies (SLHC) with less than $50 billion in consolidated assets in the population of Federal Reserve-supervised entities for which InTREx is used for evaluating IT-related risks; and
  – implement a consistent approach for Federal Reserve staff in assigning URSIT ratings.

InTREx Program Elements

- IT Profile
  - Inherent Risk Profile
  - Qualitative Adjustments

- Work Program
  - Full Work Program
    - Core Modules
    - Expanded Procedures
    - Base Work Program
  - Supplemental Modules
    - Target Work Papers
    - Cybersecurity, Gramm-Leach-Bliley Review Conclusion Memorandums

IT Profile Key Features

• Q & A Format
• Significant risk areas considered
  - Core Processing
  - Networking
  - Online Banking
  - Software Development and Technology Planning Activities
  - Responses to Software and Services Request list
• Gross technology profile score
• Qualitative adjustments
  - Unique characteristics
  - Previous examination ratings and findings
  - Enforcement actions;
  - Fraud red flags and/or customer or examiner complaints about data accuracy;
  - Concerns raised during offsite surveillance;
  - Critical service provider concerns
  - Reliance on a dominant TPSP
  - Mergers/acquisitions
Examination Procedures (cont’d)

- Each Core Analysis Decision Factor is based on assessment factors within the component rating definitions outlined in SR letter 99-8, “Uniform Rating System for Information Technology.”
- The Core Modules contain examination procedures mapped to these decision factors to facilitate the assignment of component and composite ratings.
- Examiners should check the box most representative of the assessment for that particular decision factor.
- If decision factors are completed, the following definitions should be used when rating each factor:

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong</td>
<td>Performance that is robust in nearly every respect</td>
</tr>
<tr>
<td>Satisfactory</td>
<td>Performance that provides adequately for the safe-and-sound operation of the IT department</td>
</tr>
<tr>
<td>Less than satisfactory</td>
<td>Performance that exhibits some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe</td>
</tr>
<tr>
<td>Deficient</td>
<td>Performance that results in an unsafe and unsound environment and may impair the future viability of the institution</td>
</tr>
<tr>
<td>Critically deficient</td>
<td>Performance that is critically deficient and in need of immediate remedial attention</td>
</tr>
</tbody>
</table>

Summary

- Bank management should:
  - understand inherent risk relating to cybersecurity
  - monitor and manage sufficient awareness of continuing and emerging threats and vulnerabilities
  - establish a dynamic control environment
  - involve the board of directors and senior management to provide proper oversight

Questions
Threat Intelligence Information Sources

Government and Institutional Resources
- Federal Bureau of Investigation (FBI)
- InfraGard
- United States Secret Service (USSS)
- Electronic Crimes Task Force
- Department of Homeland Security (DHS)
- United States Computer Emergency Readiness Team (US-CERT)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Financial Crimes Enforcement Network (FinCEN)
- Common Vulnerability Enumeration Database (CVE)
- National Vulnerability Database

Sector, Industry and Technology-Focused Resources
- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Competitors, partners, and financial industry associations
- Industry news sites, e.g. krebsossecurity.com, bankinfosecurity.com
- Information security sector sites, e.g. Internet Storm Center, Open Threat Exchange (OTX), ATLAS
- Managed security service providers (MSSPs) – blogs and feeds

For More Information

- FBI Alert: Fraudulent ACH Transfers
  http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm
- FDIC Special Alert: Fraudulent Electronic Funds Transfers
- FDIC Special Alert SA-185-2009 Fraudulent Funds Transfer Schemes
- NACHA Bulletin: Corporate Account Takeovers
For More Information

- FFIEC IT Handbooks: http://ffiechandbook.fdic.gov
- FFIEC Cybersecurity Awareness Web Site: http://ffiec.gov/cybersecurity.htm
- Financial Services Information Sharing and Analysis Center (FS-ISAC) www.fsicom.com/
- United States Computer Emergency Readiness Team (US-CERT) www.us-cert.gov/
- InfraGuard: www.infraguard.org/
- The Top Cyber Threat Intelligence Feeds: www.thecybertthreat.com/cyber-threat-intelligence-feeds/

Regulatory Guidance

- SR 15-3: Strengthening the Resilience of Outsourced Technology Services
- SR 15-9: FFIEC Cybersecurity Assessment Tool
- SR 12-14: Revised Guidance on Supervision of Technology Service Providers
- SR 11-9: Interagency Supplement to Authentication in an Internet Banking Environment
- SR 09-2: FFIEC Guidance Addressing Risk Management of Remote Deposit Capture
- SR 06-13: Q&A Related to Interagency Guidance on Authentication in an Internet Banking Environment

Regulatory Guidance continued

- SR 05-19: Interagency Guidance on Authentication in an Internet Banking Environment
- FFIEC Risk Management of Remote Deposit Capture
- FFIEC Information Security Booklet
- SR 01-15: Standards for Safeguarding Customer Information
- SR 01-11: Identity Theft and Pretext Calling—(attachment) Interagency Guidelines Establishing Standards for Safeguarding Customer Information
Vendor Resources & References

- Trusteer
- ThreatMetrix
- Akamai
- FBI
- enews@bankinfosecurity.com
- www.gemalto.com