Preventing For Your Next NCUA IT Exam Visit

James Harris is the CEO of Compliance Advisory Services, LLC, a nationally known information security consulting and risk management firm.

He has over 26 years of experience in the banking/credit union industry. His expertise is in all areas of information systems security, Gramm-Leach Bliley Act, PCI, and Sarbanes Oxley Act. James is former banker and FDIC examiner, with a unique ability to reduce complex legal concepts to plain English.

Easiest way to contact me: jharris@complianceadvisoryservices.com
Preparing For Your Next NCUA IT Exam Visit

James holds many cyber security certifications:

• JD Law Degree
• CISSP Certified Information System Security Professional
• CISA Certified Information Systems Auditor
• CEH Certified Ethical Hacker
• CHFI Certified Hacking Forensic Investigator
• CPT Certified Pentester
• OPST Open Source Professional Security Tester
Preparing For Your Next NCUA IT Exam Visit

• Is your credit union prepared for your next regulatory IT Exam?

• Where should you begin?

• What are the regulators going to focus on?

• What are the regulators going to ask?
Preparing For Your Next NCUA IT Exam Visit

Is your credit union prepared for your next regulatory IT Exam?

- Obtain a copy of your last Exam
- Determine all of the IT/InfoSec findings noted in the exam
- Transfer those findings onto a “tracking sheet”
Preparing For Your Next NCUA IT Exam Visit

Is your credit union prepared for your next regulatory IT Exam?

• Determine whether all prior IT Exam Findings have been corrected
• If not, correct them immediately
• If they were corrected then note that on the “tracking sheet’
• Do the same for any and all internal & external IT Audits since the last exam
Preparing For Your Next NCUA IT Exam Visit

Is your credit union prepared for your next regulatory IT Exam?

• Make sure your important policies and risk assessments are up to date.
  
  ➢ Information Security Program & Risk Assessment
  ➢ IT Policy
  ➢ E-Banking Policy & Risk Assessment
  ➢ Incident Response Plan – do not forget (DDoS & Ransomware language)
  ➢ BCP/DR Plan (test it annually)
Preparing For Your Next NCUA IT Exam Visit

Is your credit union prepared for your next regulatory IT Exam?

• Mobile Device Policy - BYOD
• Mobile Banking Policy (remember mobile deposit language & limits)
• Wire Transfer Policy – (do not forget: board approved limits)
• Instant Issue Debit/Credit Card Policy & Risk Assessment [do not forget]
Preparing For Your Next NCUA IT Exam Visit

What are the regulators going to focus on?

• Has your board received documented Cyber Security Training?
• Has your board received Cyber Intelligence Summaries on a regular basis? [FS-ISAC]
• Has your board received your GLBA Annual Status Report on the InfoSec Program?
• Do your IT Committee regularly convene (quarterly or at least 4 times a year)?
• Are your IT Committee minutes provided to the board?
• Do you have a written IT Strategic Plan (3yr forward-looking plan)?
• Have you completed a documented annual review of critical vendors?
Preparing For Your Next NCUA IT Exam Visit

What are the regulators going to focus on?

• Are you properly managing and controlling risk with all aspect of E-Banking

  ➢ Customer Authentication (MFA) – Must be MFA
  ➢ Bill Payment limits
  ➢ Wire Transfers – Out of band call-backs
  ➢ ACH Originations – time of month, typical dollar amount, number of item in file, etc
Preparing For Your Next NCUA IT Exam Visit

What are the regulators going to ask?

• Logical Controls Settings – Network, Core Banking Platform, and major Apps
  - Pwd min length?
  - Pwd complexity enabled?
  - Pwd change interval?
  - Time-out setting?
  - Lockout setting?
  - Pwd History?
Preparing For Your Next NCUA IT Exam Visit

What are the regulators going to ask?

• **Print screens of the following – Network:**
  - Screenprints showing the members of the built-in Administrator group
  - Screenprints of Domain Administrators
  - Screenprints of Enterprise Administrators
  - Screenprints showing Guest Group members & which ones have been disabled
  - Permissions for two key network shares – Accounting and HR?
Preparing For Your Next NCUA IT Exam Visit

What are the regulators going to ask

• Print screens for the following – Mainframe:

Provide a copy of the following files:

• /etc/passwd
• /etc/security/user
• /.rhosts
• /etc/hosts.equiv
• /etc/inetd.conf
• /etc/services
Preparing For Your Next NCUA IT Exam Visit

What are the regulators going to ask

• Cybersecurity Risk Assessment Tool (CAT Tool)
  ➢ How did your CU complete it? (Individual or committee)
  ➢ How long did it take to finish it? (they need a timeframe)

• The NCUA has made it a requirement to complete!

• What was your CU’s Inherent Risk? They will want to review the questions & answers
• Did you fully meet Baseline Requirements? Partial doesn’t count!!!
Preparing For Your Next NCUA IT Exam Visit

What are the regulators going to ask

- NCUA will complete several of their IT Audit Programs.

  - IT – Items Needed
  - IT – 748 Expanded (Most IT examiners complete this one)
  - IT – Anti-Virus & Malware (Optional)
  - IT – Audit Program (Optional)
  - IT – Business Continuity (Most IT examiners complete this one)
  - IT – Electronic Banking (Required)
  - IT – Networks (Most IT examiners complete this one)
  - IT – Policy Checklist (Optional)
  - IT- Firewalls (Optional)
  - IT – IDS/IPS (Optional)
  - IT – PenTest Review (Most IT examiners complete this one)
  - IT – Physical & Environment (Most IT examiners complete this one)
  - IT – Remote Access (Most IT examiners complete this one)
  - IT – Virtualization (Optional)
  - IT – Wireless Networks (Optional)
Preparing For Your Next NCUA IT Exam Visit

• Review prior IT exam results.
• Correct all prior IT Exam/Audit Findings
• Understand what IT examiners are looking for.
• Review and update all IT/InfoSec policies & risk assessments
• Ensure logical controls are appropriate.
• Understand what questions examiners will ask.
• Complete your CAT Tool.
Preparing For Your Next NCUA IT Exam Visit

Thank you for your time and attention! Good luck with your next IT exam.

James Harris, JD, CISSP, CISA, CEH, CHFI, OPST
jharris@complianceadvisoryservices.com
Austin, Texas
502-552-0559