



Common IT Audit Findings



Porter Keadle Moore, LLP

Mike Morris, CISA

Objectives

- ▲ Communication of our common IT audit findings.
- ▲ Provide a forum for you to share your recent audit experiences.

PKM's IT Audits

- ▲ Our scope follows guidance defined in the Federal Financial Institution Examination Council's (FFIEC) IT Handbooks (www.ffiec.gov).
- ▲ Common findings include what we are seeing both in audits and in recent regulatory reports issued to our banking clients.



Management

▲ Vendor Management

- ▶ Process should be formalized through policy;
- ▶ Include all critical vendors;
- ▶ Ensure that application change management is included;
- ▶ Be summarized and presented to the Board of Directors annually; and
- ▶ Include your bill pay provider.

Management, Continued

▲ Segregation of duties

- ▶ As financial institutions grow, they sometimes forget to revisit user access on critical systems.
- ▶ In organizations where segregation of duties cannot be maintained, the manual reviews must be strong.

Management, Continued

▲ Strategic Planning

- ▶ IT-specific planning is not addressed in the financial institution's strategic plan
- ▶ Reactive versus proactive – You should be considering:
 - Emerging technologies
 - New services or new ways to deliver current services
 - Are market demographics changing due to technology?
 - What does the future look like?
 - Where do technology trends appear to be heading?
 - Can our current vendors take us where we want to go?



Management, Continued

▲ Policies and Procedures

- ▶ Firewall Policy
 - All ports closed by default
 - Identify all inbound and outbound ports
 - How risks to open ports are mitigated
- ▶ Information Security
- ▶ Incident Response

Management, Continued

▲ Policies and Procedures

▶ Remote Access Policy

- How and when is it granted
- Expected security standards for approved users
- Remote access approval process

Information Security

▲ Information Security Risk Assessment

- ▶ Can be a subset of an overall IT risk assessment;
- ▶ Should include all risks associated with non-public customer information through the information's life cycle; and
- ▶ Ensure that all mitigation controls are covered by your audit process.

Information Security, Continued

▲ Information Security Program

- ▶ Information disposal should include:
 - Electronic (retired hard drives, backup media, etc.)
 - Non-electronic (sensitive reports, loan applications, etc.) formats
 - Biggest risks usually involve the human element (user security awareness testing identifies weaknesses)

Information Security, Continued

▲ GLBA Program Reporting

- ▶ Evaluate the control effectiveness of identified mitigating controls
- ▶ Communicate the results to the Board of Directors annually
- ▶ Watch out for audit gaps or overlaps



Information Security, Continued

▲ Incident Response

- ▶ Does not address the use of third-party experts (i.e. forensics experts)
- ▶ Does not address the process for how and when to file a suspicious activity report (SAR)
- ▶ Employees are not aware of their responsibilities for reporting suspicious activities

▲ Vendor Management

- ▶ Non-critical vendors may have access to non-public customer information, but have not been evaluated



Business Continuity Planning (BCP)

▲ Business Impact Analysis

- ▶ Management should prioritize and assess all business functions and processes
- ▶ Should define the maximum allowable downtime and acceptable level of losses
- ▶ Should include:
 - Recover Time Objectives (RTO)
 - Recovery Point Objectives (RPO)

BCP, Continued

▲ BCP Risk Assessment

▶ Should address:

- Human (malicious activity – hacking, intentional destruction, etc.)
- Natural Disasters (flood, tornado, hurricane, fire, etc.)
- Technical Disasters (hardware failures, power outages, etc.)
- Pandemic Incidents (H1N1)

BCP, Continued

▲ BCP Testing

- ▶ Make sure that all aspects of the BCP are tested
- ▶ Participate in third-party testing, when possible (and document it!)
- ▶ Coordinate testing wherever possible
- ▶ Ensure that all testing results are presented to the Board of Directors
- ▶ Document unscheduled tests
- ▶ Perform table-top tests, where needed

Operations

▲ Data Backup

- ▶ Tapes are not:
 - Rotated off-site timely (remember RPOs)
 - Tapes are not secured in transit
 - Tapes are not secured at the off-site location
- ▶ Tapes are exposed to extreme conditions

Logical Security

- ▲ Administrative rights not properly restricted
 - ▶ Most financial institutions should have 2-3 designated administrators per application
- ▲ Administrators are not restricted from performing transactional banking functions
- ▲ Administrative activity is not properly reviewed
 - ▶ Administrator activity logs reviewed by an administrator or not reviewed at all

Logical Security

- ▲ Preventive controls are not maximized
 - ▶ Wire transfer limits not enforced by wire application
 - ▶ Access to dormant accounts is not restricted
 - ▶ Access to sensitive network folders is not restricted
- ▲ Terminated employee access is not removed/disabled immediately upon termination
- ▲ Vendor access is not disabled after use

Questions?

Mike Morris
Systems Partner
mmorris@pkm.com
(404) 420-5669

