IT Audit for the Non-IT Auditor

Presented By

Brad Atkin, CPA, CISA, CITP, SOC – Shareholder

DoerenMayhew

IT Audit for the Non-IT Auditor

- Current knowledge and communication gap
- What are the elements?
  - Understand the Risks
  - Understand the Tests
  - Common Gaps
- What are the common findings?

IT Audits – The Elements

DoerenMayhew
CPAs AND ADVISORS

ACUIA Annual Conference - 2019

IT Audits –
The Elements

- Where to start
  - Understand your risks
  - Know the tests
  - Understand the value

IT Audits – The Elements

- Understand your risks (Risk Assessment)
  - FFIEC – “understand and evaluate…definitions and categories”
  - Operational risk is highly affected by IT
  - Methodology
    - Identify key systems
    - Assess risk with criteria (consider control methods)

IT Audits – The Elements

- Understand your risks (Risk Assessment)

Data Classification								Weighted Risk Summary
Information Category	Critical Asset/Container	Public	Sensitive	Confidential	Ownership	Criticality		100%
Network and Network Infrastructure	Network Servers - High Risk	X	X	X	IT	H		24.5
Operating systems	Microsoft Network		X	X	IT	M		23.4
Operating systems	VMware		X		IT	H		23.4
Network and Network Infrastructure	VoIP Phone System	X	X	X	IT	H		23
Network and Network Infrastructure	Firewall and VPN		X	X	IT	H		22.4
Data Sharing	Exchange Server - 2016		X	X	IT	M		22.4

IT Audits – The Elements

- Understand your risks
  - Make strategic decisions
  - Balance risk and control investments
  - Assurance on management of IT risk
  - Auditors/Regulators understand risk and control environment

Risk by Category	Weighted Average by Category
Information Category	100%
Loans Total	21.5
Operating systems Total	21.4
Network and Network Infrastructure Total	20.0
Member Data Total	17.1
Core System Total	16.6
Data Sharing Total	14.0
Mortgage system Total	13.8
Financial Systems Total	12.3
Communications Total	10.4
Monitoring Total	9.1
Physical and Environmental Total	9.0

IT Audits –
The Elements

- Understand your risks (Risk Assessment)
  - Better process yields better strategy
  - Develop a proper rotation
  - Select the right vendor

IT Audits –
The Elements

- Understand the tests – IT General Controls
  - IT Management and Governance (involvement, responsibility, strategy, HR)
  - Change Management and Program Maintainability (initiate, review, approve, assess, policy, patching)
  - IT Operations and Backup (schedule and test)

IT Audits –
The Elements

- Understand the tests – IT General Controls
  - Logical Access Control (user access, admin, password, external, least privilege)
  - Segregation of duties (admin, loan approval)
  - Physical security (access, threats)

IT Audits –
The Elements

- Understand the tests – IT General Controls
  - Network Infrastructure (anti-virus, firewalls, routers)
  - Business Continuity and Disaster Recovery (plan, test, approve)
  - Internet Banking (application, origination, activity, multifactor)
  - Mobile Banking (remote disable, interception, privilege escalation)
  - Remote Deposit Capture (compliance, access, activity)

IT Audits – The Elements

- Understand the tests – GLBA
  - Comprehensive Information Security Program
  - Review Info Risk Assessment
  - Vendor Management (due diligence)
  - Intrusion Detection/Incident Response (assessment, notification)
  - Encryption Methodologies
  - System and Media Destruction (disposal, transit)

IT Audits – The Elements

- Understand the tests – Vulnerabilities
  - External scan
  - Internal scan (with credentials)
  - Penetration Testing

IT Audits – The Elements

- Common Gaps in Proposals and Plans
  - Internal Vulnerability scans not credentialed
  - Ignoring applications
  - Logical access not performed
  - Testing of areas only includes policy review

IT Audits – The Findings

DoerenMayhew CPAs AND ADVISORS

ACUIA Annual Conference - 2019

IT Audits – The Findings

Area Tested	Heading	IT Audit Finding	Risk to CU	Solution
GLBA	Hardware/Software Inventories	The CU does not maintain a current inventory of all hardware and software it currently uses.	Per GLBA guidance, financial institutions should maintain a close physical inventory of all computer hardware.	Updating current inventory to include all hardware and software components.
GLBA	Information Security Policy	The current password policy described within the Credit Union's Information Security (IS) policy does not conform to best practice controls over password parameters.	Weak passwords can make it easy for user accounts to be compromised by hacking or password guessing.	Revise current policy to include best practice definitions of strong passwords, (minimum of 8 characters with 3 of the 4 character types, 12+ remembered, minimum age of 1 day, and maximum age of 90 days)
GLBA	End-of-Life System	The Credit Union is still running systems on Windows Server 2003.	Windows stopped providing extended support for Windows Server 2003 in July 2015. Microsoft will no longer provide fixes and patches for known vulnerabilities.	Developing and implement a plan to migrate off Windows Server 2003.
Information Technology General Controls	Network Monitoring	The Credit Union does not currently employ comprehensive network monitoring.	Should someone gain access to the internal network they would have unhampered access to ping and probe the various internal servers, hardware and computers running on the network without alerting IT staff.	Select an appropriate vendor to perform monitoring.

IT Audits – The Findings

Area Tested	Heading	IT Audit Finding	Risk to CU	Solution
Vendor Management	Complementary User Entity Control Review	The CU is not currently reviewing the complementary user entity controls within the SOC 1 report as part of the Vendor Management due diligence process for the core vendor.	The CU is responsible for reviewing and implementing all applicable controls. Without the complementary user entity controls, the controls will not operate as intended, thus potentially producing material weaknesses.	Review the complementary user entity controls and ensure they have been implemented at the CU to gain comfort the controls put in place at the service organization are operating effectively.
Incident Response	DDoS Readiness Procedures	The Incident Response Policy does not include readiness procedures related to a Distributed Denial-of-Service (DDoS) attack.	DDoS attacks may present a variety of risks, including operational risks and reputation risks. If the attack is coupled with attempted fraud, a financial institution may also experience fraud losses as well as liquidity and capital risks.	Include DDoS readiness into the current IR policy including: 1. Monitor traffic to website; 2. Activate plans and notify service providers if you suspect an attack. 3. Ensure sufficient staffing
Virus Protection	Active At-risk Clients	DM identified several active clients that are not currently protected with Endpoint Protection.	Unprotected machines become more susceptible to malware infection and put the Credit Union and member data at risk of unauthorized access or disclosure.	Ensure all active endpoints are protected with anti-virus, that virus definitions are up-to-date, and a follow up is performed when definition updates fail or have not been performed on endpoints.

IT Audits – The Findings

Area Tested	Heading	IT Audit Finding	Risk to CU	Solution
Firewall	Firewall Redundancy	The Credit Union does not have any redundancies in the firewall configuration.	Redundant firewall benefits include greater performance, fault tolerance and load balancing, enhanced security, enhanced perimeter protection, protected subnets, and failover.	Consider implementing redundant firewalls to further protect the network from unauthorized activity.
Firewalls	Firewall Change Alerts	Alerts are not currently generated when a change is made to the rule set.	Without alerts generated when a change is made to the firewall, there is a risk that unauthorized or erroneous changes will be made within the Firewall that will not be detected in a timely manner.	Utilize automated alerts to notify IT staff of important events.
Business Continuity	Business Continuity Plan Test	The Credit Union does not have a formal process to periodically test its Business Continuity Plan and ability to restore data from backups.	Periodic testing minimizes the risk of recovery and impact to the Credit Union in the event of an outage of one or more mission critical systems, which could cause a significant loss of revenue and irreparable damage to long-term member relationships.	Perform Business Continuity tests annually; procedures should include testing for the core and other critical systems, which includes practice scenarios engaging the business units for testing.

IT Audits – The Findings

Area Tested	Heading	IT Audit Finding	Risk to CU	Solution
Patch & Change Management	Lack of Test Environment	The Credit Union does not currently have a test environment.	Without a non-production environment to test changes, there is risk a change could adversely affect systems.	Add a separate non-production environment to test changes before moving to production.
Change Management - Review	Changes made to the database are not reviewed for appropriateness.	Although access is limited, the changes made directly to the database could result in unauthorized or erroneous changes. Which can lead to improper application functionality that may not be identified in a timely manner.	All database queries (that update information) or changes made directly to a table should be supported by documentation. The CU should review these data changes to detect unauthorized or erroneous changes.	All database queries (that update information) or changes made directly to a table should be supported by documentation. Celink should review these data changes to detect unauthorized or erroneous changes.
Physical and Environmental	Water Sensors	The Credit Union does not have water sensors in the server room.	Water damage from leaking pipes, air conditioning units, etc. could cause significant damage to computing equipment considering the Credit Union would not be able to respond timely.	Install water sensors beneath air conditioning vents/units, sprinkler heads/pipes, and near other possible sources of water to allow an administrator to be notified of possible water buildup prior to possible damage to server room equipment.

IT Audits – The Findings

Area Tested	Heading	IT Audit Finding	Risk to CU	Solution
Document & Media Disposal	Hardware Disposal	The Credit Union has not developed a formal process for logging the disposal of hardware that may contain sensitive data e.g. hard drives.	Per FFIEC guidance, management should log the disposal of sensitive media, especially computer-based media.	Develop procedures that record the following: • Responsible party for and performing disposal • Date • Media type • Hardware serial number • Method of disposal
Physical & Environmental	Logging vendors	Logs are not kept when outside vendors come to service equipment within the data center.	If a system problem arises soon after maintenance of equipment in data center, no audit trail exsists to hold vendors accountable.	Logs be maintained for services performed on equipment, and scheduled maintenance.

IT Audits for the Non-IT Auditor

- Takeaways
  - A robust risk assessment drives the process
  - The audit approach should match your risks
  - Significant value to going beyond the policies
  - Ask until you understand

Thank You!

Brad Atkin
Shareholder
Atkin@Doeren.com
248.244.3091

DoerenMayhew
CPAs AND ADVISORS