

IT Audit for the Non-IT Auditor

Presented By

Brad Atkin, CPA, CISA, CITP, SOC
Shareholder, IT Advisory and Security Group




Insight. Oversight. Foresight.®





IT Audit for the Non-IT Auditor

Goals for the Session

- 
- 1 Understand the **expectations**
 - 2 Get to know the **elements** and **gaps**
 - 3 Appreciate the **value** proposition
 - 4 Find some nuggets to bring back home



Expectations

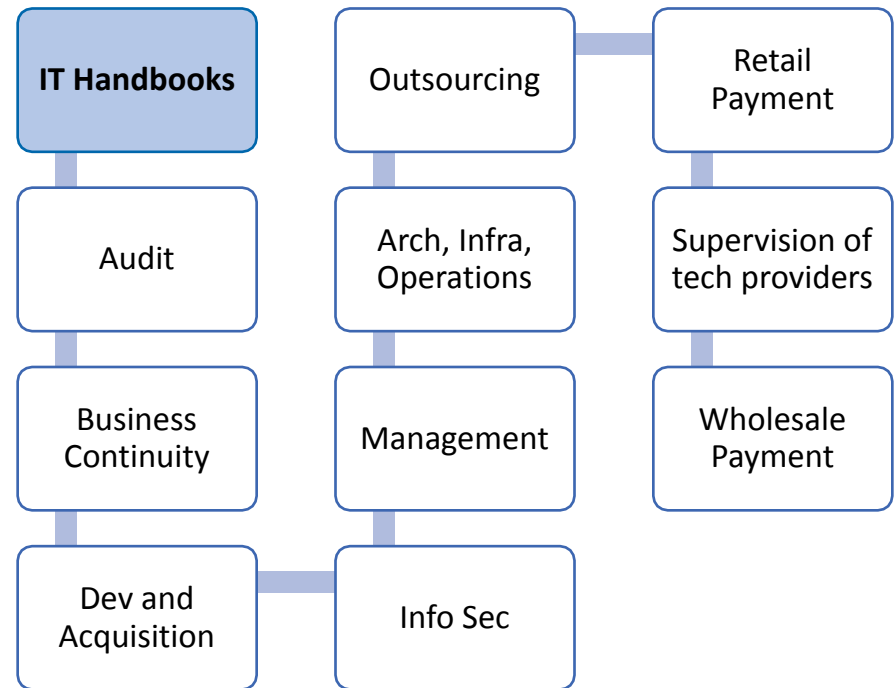
Expectations – NCUA & FFIEC

Regulators
expect CUs
to address

- Information Security Risk Assessment
- Effectiveness of IT Controls (Are they designed well and working?)
- Vulnerability Management (scans, penetration testing/hacking, remediation)
- Compliance (ex. GLBA)

Expectations – NCUA & FFIEC

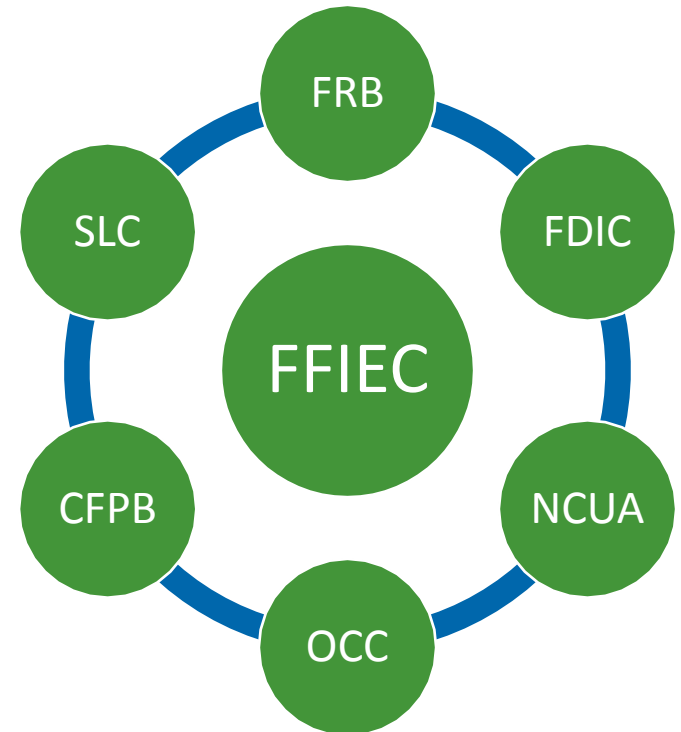
- IT Audits address **effective risk management**
- Guidance through **IT Examination Handbooks** (ithandbook.ffiec.gov)
 - Best practices and expectations
 - Sound IT governance, risk management, security practices
 - Protect member info, ensure op resilience, comply with laws and regs



Expectations – NCUA & FFIEC

- FFIEC Resources

- Cybersecurity Resource Guide (Revised Nov 2022)
- Cybersecurity Assessment Tool (inherent risk and cyber maturity)
- IT Booklets and IT Work programs



Expectations – NCUA & FFIEC

- Internal IT Audit Staff Roles and Responsibilities
 - Evaluate (plans, strategies, policies, procedures)
 - Assess day-to-day IT controls for **transactions** (recording, processing, financial reporting, compliance)
 - Involved in **development** process for major new IT apps
 - **Criteria** for whether projects need audit involvement (new apps, products, conversions)

Expectations – NCUA & FFIEC

- Additional Risk-Based Elements

- Identify audit universe (data, apps, O/S, tech, facilities, personnel, business activities)
- IT Risk Scoring ->

Age of system/app

Complexity

Operating environment

- Changes in volume
- Centralization
- Sensitivity
- \$ impact
- Conversions

Physical & logical security

Previous findings

HR

- Mgmt experience/competence
- Turnover

Expectations – NCUA & FFIEC

- Understand your risks

- Risk-based rotation
- Availability vs external scoping
- Expertise
- Map to audit plan
- Balance risk
- Control investments

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

Expectations – Risk-Based Plan

IT Risk-Based Audit Matrix									
Audit Area	Inherent Risk	Residual Risk	Risk Direction	Frequency	Last Audit				Performance
	L/M/H	L/M/H	Down/=/Up	L/M/H		2023	2024	2025	Int/Ext
GLBA	High	Moderate	Down	Moderate	2022		X		DM
IT Management and Governance	Moderate	Moderate	=	Moderate	2021	X		X	Internal
Change Management and Program Maintainability	High	Moderate	=	Moderate	2022		X		DM
Project Management	Moderate	Moderate	=	Moderate	2022		X		DM
Data Analytics and Management	Moderate	High	Up	High		X	X	X	DM
IT Operations	Low	Low	=	Low	2021		X		Internal
IT Backups	Moderate	Moderate	=	Moderate	2021		X		DM
Segregation of Duties	High	High	=	High	2022	X	X	X	DM
Physical and Environmental Security	Low	Low	Up	Moderate	2021	X		X	DM
Network Infrastructure									
Anti-Virus Protection	High	Moderate	=	Moderate	2022	X		X	DM
Firewalls and Routers	High	Moderate	=	Moderate	2022	X		X	DM
Wireless Networks	High	Moderate	=	Moderate	2022		X		DM

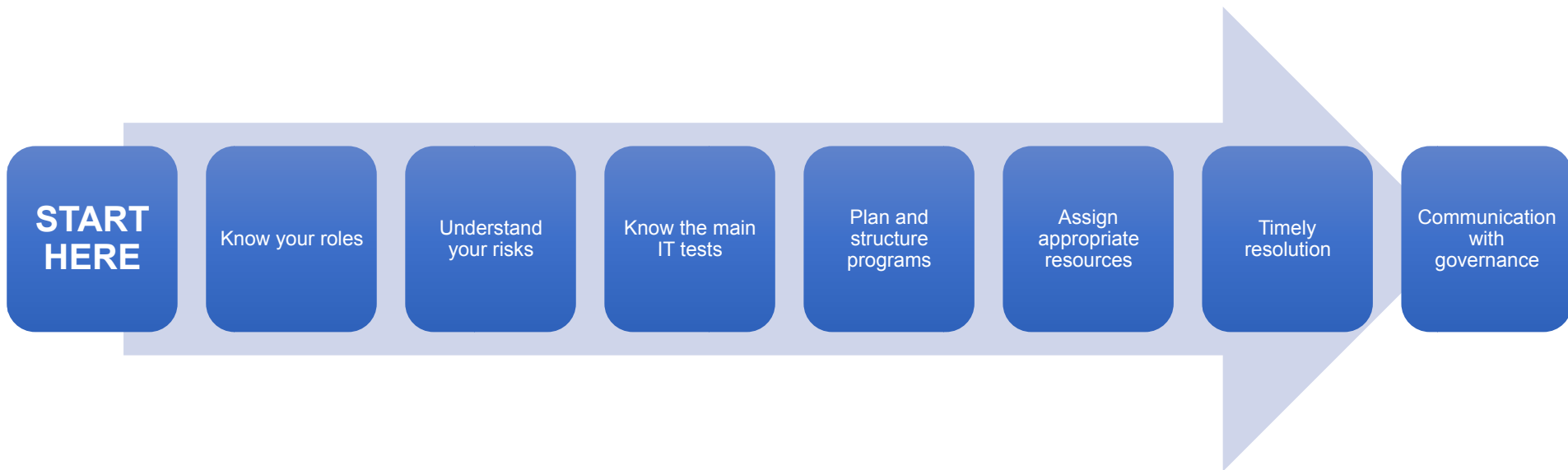
Expectations – NCUA & FFIEC

- Outsourced IT Internal Audit
 - All or some, but still **managed/overseen** by internal auditor or audit committee
 - Contract requirements: Protocol for **changing services** due to risk/environment
 - Provider can help with **risk determinations** due to expertise
 - Work together on **rating** findings (industry expertise)
 - Proper **due diligence** (skills, knowledge, expertise)



The Elements

The Elements



The Elements – The Tests

IT General Controls/ITGC

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)

Logical Access Control (user access, admin, password, external, least privilege)

Segregation of duties (admin, loan approval)

The Elements – The Tests

IT General Controls/ITGC

Physical security (access, threats)

Network Infrastructure (anti-virus, firewalls, routers)

Business Continuity and Disaster Recovery (plan, test, approve)

Internet Banking (application, origination, activity, multifactor)

Remote Access (remote disable, interception, privilege escalation)

The Elements – 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)

The Elements – The Tests

Vulnerability
Management

Identify and assess
weaknesses in system

External scan (test where you are
open to internet)

Internal scan (in network with
credentials)

Penetration Testing
("Ethical Hacking")

Patch, update software,
reconfigure systems

The Elements – The Gaps

Internal
Vulnerability scans
not credentialed

Ignoring
applications

Logical access not
performed

Testing of areas
only includes
policy review

Limited IT
expertise

Lack of industry
knowledge or
operational goals

All scopes are the
same (no risk
adjustments)

Segregation of
duties



The Value Proposition

The Value Proposition – Third Party

- Solving the large **expertise gap** (cost share of vast expertise needed)
- Strategic **partners** - Findings, recommendations, best practices, advisory, communication, advocacy
- Wide **industry** knowledge (risks, controls, tools, core, operations)
- Assist your **fiduciary duty** to members

The Value Proposition – Third Party

Known in industry

More than policies

Diverse expertise

Thought leader

Risk-based scope

Clear communication



Questions?



Brad Atkin, CPA, CISA, CITP, SOC

Shareholder, IT Advisory and Security Group

248.244.3091

atkin@doeren.com

Thank You!