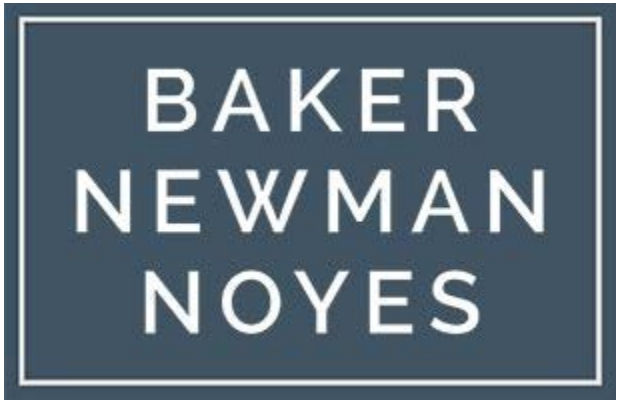
BAKER NEWMAN NOYES

Hot Topics for Banking Executives

October 14, 2015



ASSESSING CYBER RISKS

Current Trends and The New FFIEC Cybersecurity Assessment Tool

Patrick Morin, CPA, CISA, CISM, CITP, Risk & Business Advisory Principal

Goals For The Session

Presentation Checklist:

- Trends in Cyber Risks
- FFIEC Cybersecurity Assessment Tool
- The Two Parts of the FFIEC Tool
- Using the FFIEC Tool

Trends in Cyber Risks

- Existing vulnerabilities continue to be exploited
- New platforms create new cyber attack opportunities
- Lines between cyber actors are blurring
- Tactics evolve in response to online behavior
- Trends in malware are evolving
- Global threats continue to grow

Trends in Cyber Risks

The volume of cyber attacks are rising

- Annual Attack volume has risen by 176% in the past 5 years thanks to automation
- Various studies indicate that over 80% of employees are unable to detect common attacks, such as phishing scams
- 18% of phishing email recipients click the link
- Global cost of cyber crime in 2014 was between $375 and $575 Billion
- Studies have found financial institutions have substantially higher annual costs associated with cyber crime relative to other industries
- 80% of financial institutions have had a cyber security incident

Trends in Cyber Risks

Social Engineering Tactics

- Mimicking sender domain names; e.g pmorin@bnncpa.com vs. patmorin@bnmcpa.com
- Reciprocation: giving the target something in order to make them feel obligated to return the favor
- Scarcity: giving the target a limited timeline for acting or face adverse consequences. e.g. “I need this information to get our website back online, NOW!”
- Consistency: hackers have begun to build a rapport with targets to build trust over several emails and/or phone calls. e.g. pretending to be a member of the IT department with a mimicked email

FFIEC Cybersecurity Assessment Tool

FFIEC Cybersecurity Assessment Tool

Objective From the FFIEC:

To help institutions identify their risks and determine their cybersecurity maturity. The Assessment provides institutions with a repeatable and measureable process to inform management of their institution's risks and cybersecurity preparedness.

The Tool Aims To:

- Help institutions identify their cyber risks
- Determine their cyber security preparedness
- Assess whether an institution’s preparedness is aligned with its risks
- Outline necessary risk management practices and controls

FFIEC Cybersecurity Assessment Tool

The tool is consistent with practices from:

- FFIEC Information Technology Examination Handbook (IT Handbook)
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Industry accepted cybersecurity practices

The Two Parts of the FFIEC Tool

The Two Parts of the FFIEC Tool

The assessment is separated into two parts:

- 1. Measuring an institution's Inherent Risk
- 2. Assessing The Maturity of its Cybersecurity program.

- The structured approach will allow banks to better understand the key drivers of cyber risks and important controls for mitigating the risks

- The tool also aggregates its findings so that business leaders can make better informed decisions

The Two Parts of the FFIEC Tool

Inherent Risk Measurement

- Helps an institution evaluate the likelihood of an attack on their systems.

- The assessment tool recommends the following five areas to evaluate, separately, on a scale from least inherent risk.

    - Technology and Connection Types
    - Delivery Channels
    - Online/Mobile Products and Technology Services
    - Organizational Characteristics
    - External Threats

The Two Parts of the FFIEC Tool

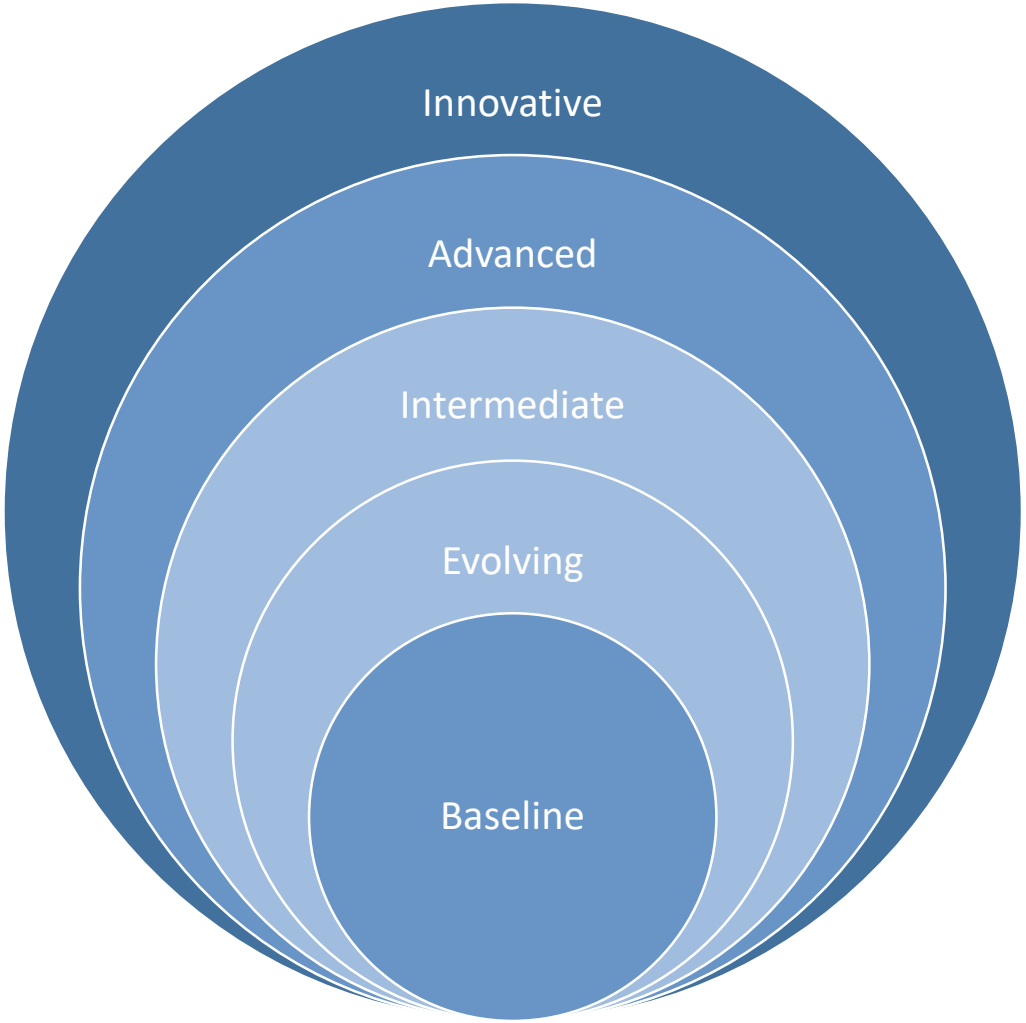
Cybersecurity Maturity

The tool helps institutions evaluate their security program by reviewing their policies and controls across five domains and corresponding components:

Domain 1: Cyber Risk Management & Oversight	Domain 2: Threat Intelligence & Collaboration	Domain 3: Cybersecurity Controls	Domain 4: External Dependency Management	Domain 5: Cyber Incident Management & Resilience
• Governance • Risk Management • Resources • Training and Culture	• Threat Intelligence • Monitoring and Analyzing • Information Sharing	• Preventative Controls • Detective Controls • Corrective Controls	• Connections • Relationship Management	• Incident Resilience Planning and Strategy • Detection, Response, and Mitigation • Escalation and Reporting

The Two Parts of the FFIEC Tool

Maturity Levels



Using The FFIEC Tool

Using the FFIEC Tool

Measuring Inherent Risk Combines both Qualitative and Quantitative Measures

Figure 1: Inherent Risk Profile Layout

Risk Levels

Activity, Service, or Product

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

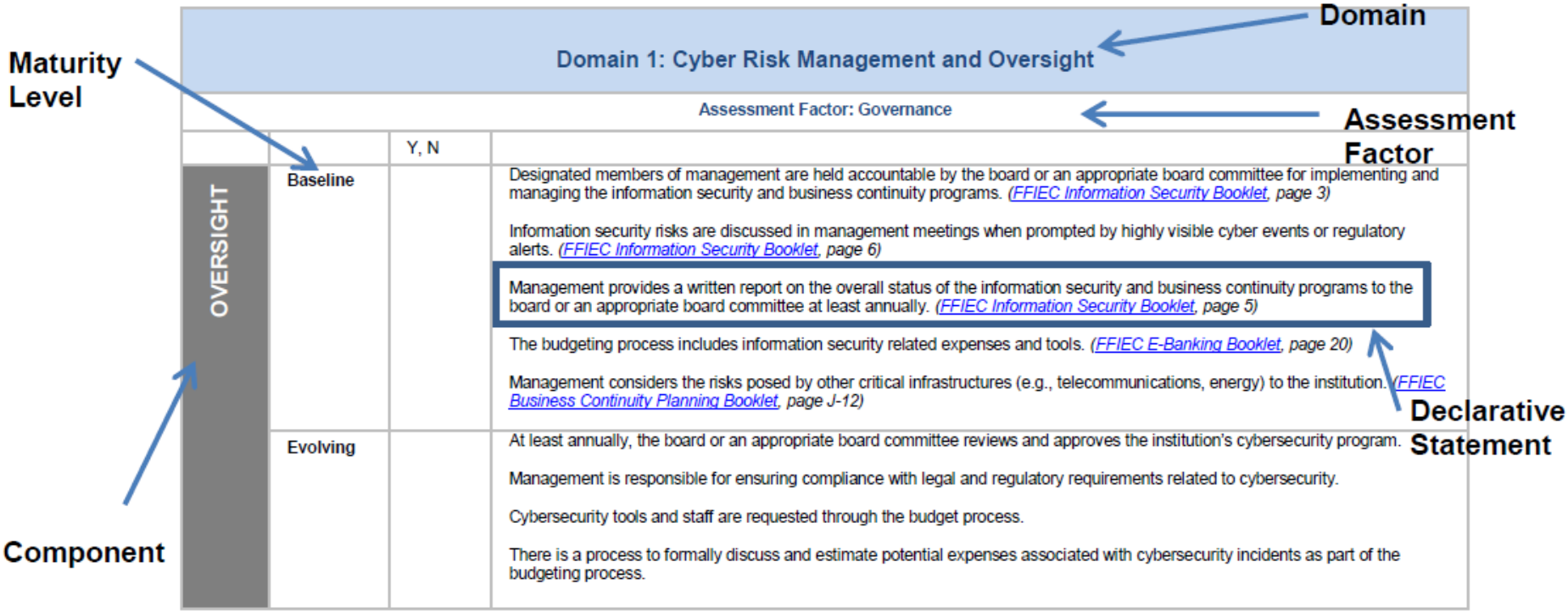
Figure 2: Inherent Risk Summary

	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Number of Statements Selected in Each Risk Level	4	8	25	2	
Based on Individual Risk Levels Selected, Assign an Inherent Risk Profile	**Least**	**Minimal**	**Moderate**	**Significant**	**Most**

Using the FFIEC Tool

Assessing Cybersecurity Maturity

Figure 4: Cybersecurity Maturity



Using the FFIEC Tool

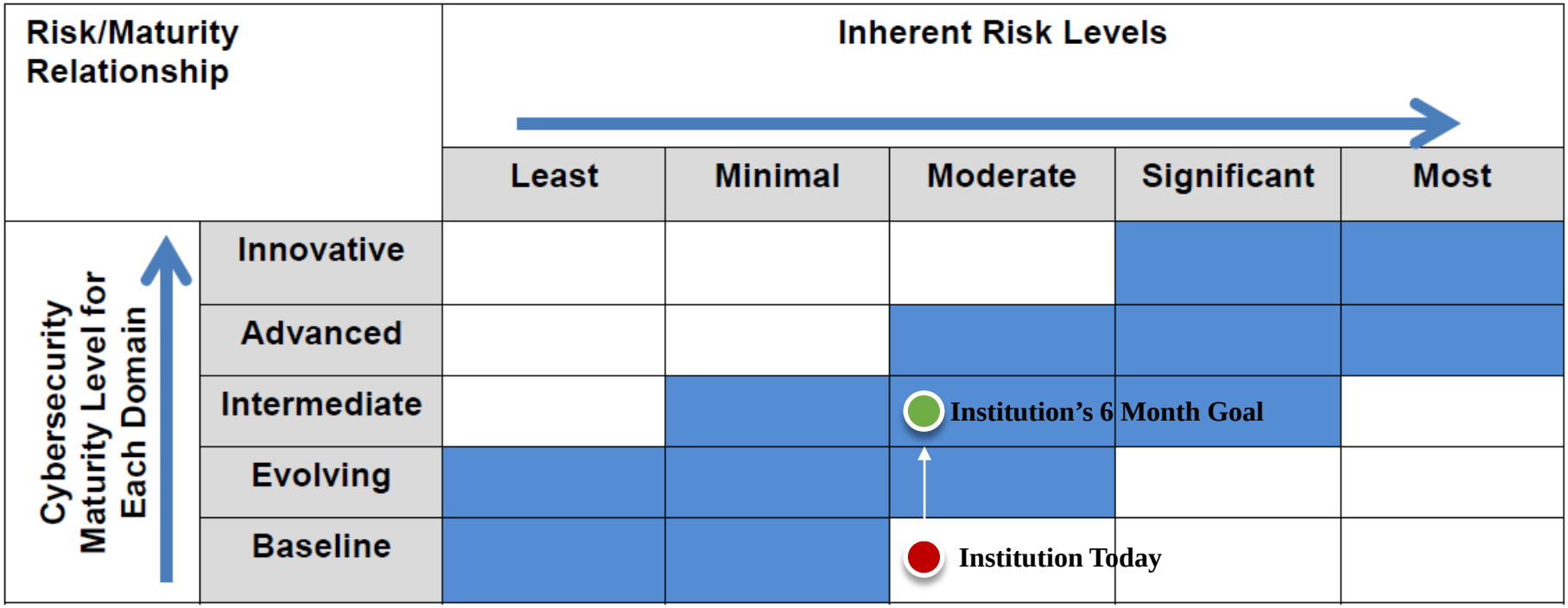
Risk Appetite

Ultimately, the assessment gives business leaders the data they need to determine their “Risk Appetite”

- Business leaders must determine how much exposure to unmitigated cyber risk they are comfortable with
- This should be a function of likelihood of attack, cost to the organization, and cost to customers
- Risk Appetite and Inherent Risk should be considered together to make a decision about balancing the cost of implementing security programs with different levels of maturity versus the potential cost of a successful attack

Using the FFIEC Tool

After evaluating Inherent Risk, Risk Appetite and current Cybersecurity Maturity, an institution can use the matrix below to evaluate their cybersecurity program and develop goals for improvement.



Using the FFIEC Tool

Cyber Incident Management and Resilience

Planning Component

Baseline	The response team includes individuals with a wide range of backgrounds and expertise, from many different areas within the institution (e.g. , management, legal, public relations, as well as information technology). (*FFIEC Information Security Booklet*, page 84)
Evolving	Alternative processes have been established to continue critical activity within a reasonable time period.
Intermediate	A direct cooperative or contractual agreement(s) is in place with an incident response organization(s) or provider(s) to assist rapidly with mitigation efforts.
Advanced	Multiple systems, programs, or processes are implemented into a comprehensive cyber reliance program to sustain, minimize, and recover operations from an array of potentially disruptive and destructive cyber incidents.
Innovative	The incident response process includes detailed actions and rule-based triggers for automated response.

Using the FFIEC Tool

Responsibilities Within The Institution

Senior Leadership – The FFIEC has recommended that senior leaders, specifically the CEO, take responsibility for completing this assessment and determining their institution's "Risk Appetite" and implementing the appropriate Cybersecurity program.

What does this mean?

This means companies must institute a security program from the top down, ultimately leaving senior management responsible for the impact of a successful attack and creating more accountability.

- Senior business leaders must be confident in the advice and data they receive from internal staff in order to make the best decision about cyber security
- Senior business leaders should on occasion seek third-party advice to validate their internal staff's work
- Senior business leaders must constantly evaluate the affect of changing business strategy and growth on the institution's Inherent Risk profile and appropriate Risk Appetite
- This sets the stage for future accountability for cybersecurity with senior-level executives

Using the FFIEC Tool

Benefits to Institutions

- 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 could be enhanced and actions that could be taken to achieve the institution's desired state of cyber preparedness.
- Informing risk management strategies.

Example: Delivery Channels

Case: Evaluating Inherent Risk Associated With a Bank's Delivery Channel

Bank: Riverbend Bank
Employees: 85
Assets: $900 million
Customers: 33,000
Scenario: Riverbend Bank is a medium sized regional bank that has typically relied heavily on it branches to deliver its banking services. Recently, the board decided to expand its internet banking capabilities with online bill pay, remote deposit, and mobile banking. Conveniently, they have found a vendor that will help them implement software in each area.

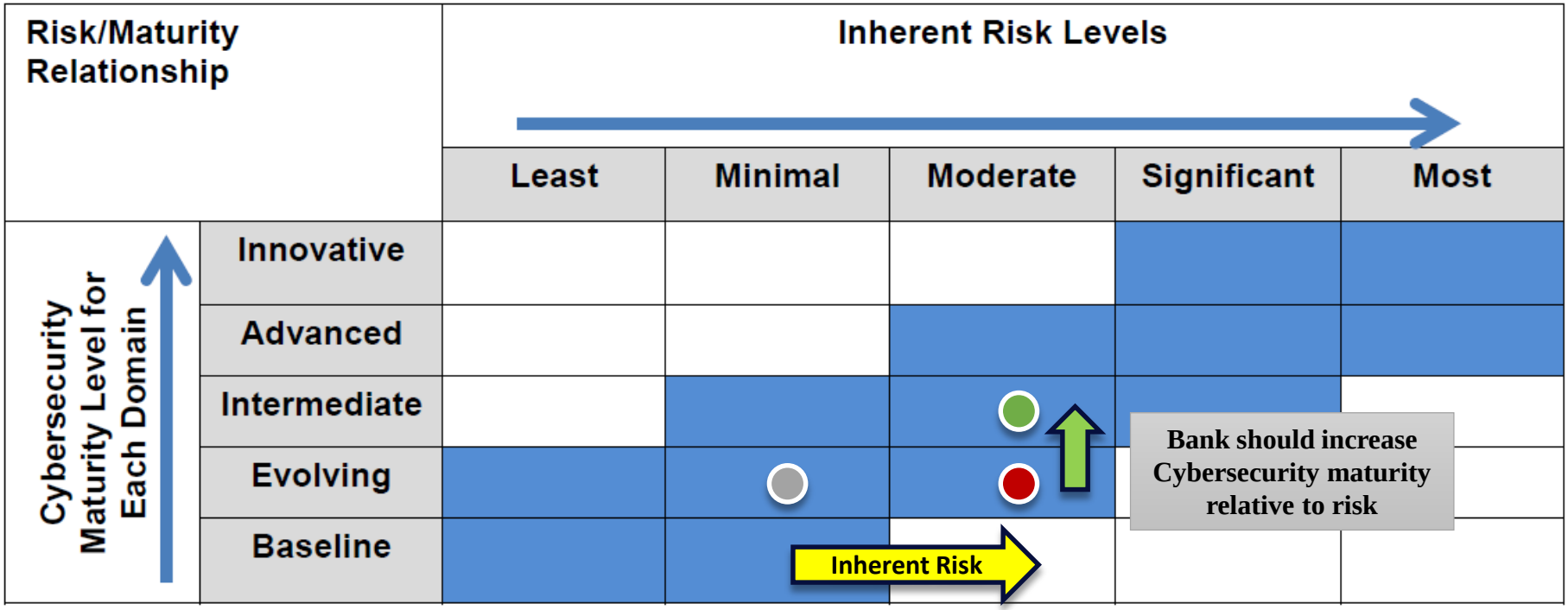
Observations: The bank is expanding the channels in which it will deliver its services to customers. As the number of channels grows, so do the opportunities for cyber criminals to conduct fraud.

Example: Delivery Channels

Case: Evaluating Inherent Risk Associated With a Bank's Delivery Channel

Effect on Inherent Risk: Significantly Increased

Effect on Cybersecurity Maturity: As the bank's Inherent Risk increased, the tool suggest that further risk mitigation should be put in place to increase the Cybersecurity Maturity Level



Questions?

BAKER NEWMAN NOYES

HOW TO:

Avoid Common 401(k) plan errors

Matt Prunier, CPA, Audit Senior Manager

Fiduciary Responsibility

Over reliance on service providers is common

Remember the plan administrators are ultimately responsible for the operations of the plan

Stay involved

- Plan committee
- Review of participant reports and investment statements
- Fees
- Investment selections (not too many)

Follow the Plan Document!

Definition of compensation

- Bonuses
- Imputed amounts
- Any irregular payments
- New pay codes

Be careful with new adoption agreements, restated plans, and plan amendments.

Loans

- Proper rates
- How many outstanding at once

Late Contributions

As soon as reasonably segregated, but no later than the 15th day of the following month.

Safe harbor for small plans

- 7 days from withholding

No safe harbor for large plans

- Sooner is better
- Consistency is important

Questions?

BAKER NEWMAN NOYES

State Tax Considerations

When Doing Business in Multiple States

Merrill Barter, CPA, Tax Senior Manager

Doing Business in Multiple States – Taxes!

Many financial institutions (FIs) do business in multiple states. Management must be aware of the states' varying laws regarding when income or other state filings are required.

For a state to impose tax, the taxpayer must have "nexus" – the requisite connection between the taxpayer and the state for the state to have the authority to tax it.

In a growing number of states, the existence of loans secured by real estate or tangible personal property (TPP) creates "nexus" – and thereby a filing requirement – for the institution.

Doing Business in Multiple States – Taxes!

Does your Institution conduct any of the following activities outside your home-state?

- Make loans secured by real estate – this could be a loan to a client for a 2nd home, or for commercial property.
- Make loans secured by TPP, including business equipment or automobiles.
- Have employees or independent contractors acting on behalf of the institution soliciting clients, negotiating loan terms or attending loan closings.

Depending on the state and level of activities, the above can result in state tax filings being required.

State Taxes – Nexus – Secured Loans

The existence of loans secured by real estate and/or TPP may create nexus, and therefore a filing requirement, in the following states (partial list):

- *Connecticut*
- *Florida*
- *Georgia*
- *Massachusetts*
- *New Hampshire*
- *New Jersey*
- *New York*
- *North Carolina*
- *Pennsylvania*

State Taxes – Nexus

In some states, when determining if an entity has a filing requirement, other factors will be considered in conjunction with the existence of secured loans, including:

- The volume of loans made
- The amount of interest income being derived from the loan
- In-state activities of employees and/or independent contractors

State Taxes – Nexus – Examples

Some specific examples:

- *Connecticut* – an FI with no office or employees in CT but that actively solicits CT residents or has significant receipts from CT customers may have nexus. Factors considered would be the number of loans, frequency of in-state visits (solicitation), and the income related to the loans. If no active solicitation exists, nexus exists if revenue from loans to CT customers is equal to or greater than $500K ("bright line" test).

- *Florida* – "doing business" includes the making of loans secured by real estate or TPP.

- *Massachusetts* – nexus for the Financial Institution Excise Tax exists if the FI regularly receives interest income from loans secured by TPP or real property located in Massachusetts

State Taxes – Nexus – Examples

More specific examples:

- *New York* – starting 1/1/2015, interest from loans secured by real property located in the State are included in the numerator of the apportionment factor. Also as of 1/1/15, the State has a "bright-line" nexus threshold of $1M of receipts from NY sources.

- *North Carolina* – nexus exists when there is more than $5M of loans secured by real property in NC and services are provided in the State. "Services in NC" is defined very broadly and includes "promoting, protecting, establishing, or maintaining the market for potential or existing customers in this State."

- *Pennsylvania* – beginning in 2014, doing business includes having $100K or more of gross receipts from Pennsylvania customers. Gross receipts specifically includes interest from loans secured by real or personal property in Pennsylvania.

State Taxes – Apportionment of Income

What's the tax impact of having to file in multiple states?

- In a perfect world, the amount of state tax an FI owes can be viewed as a pie, and each state wants its share.

- Unfortunately, due to the states' varying taxes, apportionment methods and rates, having to file in multiple states often results in a greater state tax liability.

Examples of State Apportionment Methods:

- Connecticut: sales only

- Massachusetts: 3-factor (sales, payroll and property)

- New York: sales only

State Taxes – Apportionment of Income

Example:

- FI located in Massachusetts – no other locations (all payroll and property in MA)
- Total interest from loans secured by real estate and TPP of $20M – $10M from MA, $5M from CT, and $5M from NY.
- CT and NY use only the sales factor, so the apportionment factor in each state would be 25%.
- MA uses a 3-factor formula – its apportionment factor would be 83.3% ((50% sales + 100% payroll + 100% Property) / 3)
- The result is that the FI is effectively taxed on 133.3% of its state taxable income

State Taxes – Nexus – Other Considerations

Conducting other activities within a state besides the making of secured loans can create nexus, including (partial list):

- Having a business location in the state
- Having employees, representatives or independent contractors conducting business activities in the state on behalf of the FI
- Maintaining, renting or owning any tangible or real property in the state
- Regularly performing services in the state
- Regularly soliciting and receiving deposits from customers in the state
- Ownership interests in real estate partnerships with in-state property

What if the FI Should've Filed in a State But Didn't?

Voluntary Disclosure Programs

Programs available in most states for income and other taxes whereby the state will agree to let the taxpayer "come in" to the state voluntarily and will only impose back taxes for a limited look-back period (typically 3-4 years) even if the taxpayer has been doing business in the state for longer.

Benefits: typically abatement of penalties (sometimes interest) and limited look-back; FI can file amended returns in other state(s) where the statute of limitations is open to recover some taxes.

Typically administered by a specific unit within each department of revenue (e.g., "nexus unit")

Applications are anonymous (in most cases) and can be withdrawn if state position is unfair (prior to disclosure of the client's name)

BEWARE: If the FI is "found" on audit, the state can go back to the first year the FI had in-state activity! And the FI may not have the ability to amend returns and recover taxes from other states.

Questions?