

**REDEFINING YOUR BSA AUDIT, RISK ASSESSMENT AND CONTRACT REQUIREMENTS:
FROM METHODS TO MERGERS**

5th Annual Conversation on Compliance

Marvin Johnson, CAMS, CFE AuditLink Assistant Manager
Patrick Sickels, Internal Auditor
Jim Vilker, CAMS, NCCO VP of Professional Services

1

The contents of this presentation are intended to provide you with a general understanding of the subject matter. However, it is not intended to provide legal, accounting, or other professional advice and should not be relied on as such.

2

IT ALL STARTS HERE

- The risk assessment should be considered the foundation of a compliance program.
- Without a comprehensive risk analysis of its business, it is highly unlikely that a financial institution can design an effective program well suited to manage the risks of that particular institution.

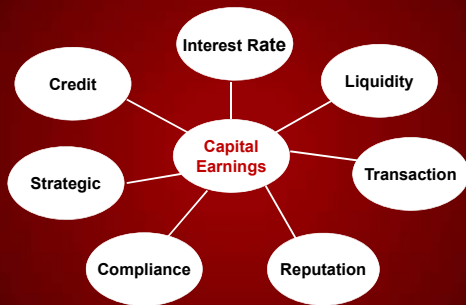
3

FLEXIBILITY IS KEY

- There is no “one-size fits all” approach to developing this assessment
- Beware of “cookie cutter” solutions

4

RISK CATEGORIES



5

RISK RESPONSE

- **Accept**
 - Risks that fall within the organizations **risk appetite** and/or that do not significantly threaten the organizations **business objectives** can be accepted
 - Laziness or apathy is not a sufficient reason to accept
- **Transfer (Reassign)**
 - Typically done through insurance
- **Mitigate**
 - Risks that cannot be accepted or realistically transferred should be mitigated through the use of control measures
- Remaining risk is “residual risk”

6

COMPLIANCE RISK

Risk of violations and noncompliance with laws, rules, regulations, or ethical standards, resulting in fines, penalties, or damages.

Impacted by:

- Regulatory requirements that impose greater responsibilities for institutions and their staff and resources. Material growth in particular areas, products, and services; or offering of new services, products, and programs.

Indicators:

- Authority and accountability
- Level of violations or noncompliance
- Training and resources
- Litigation and complaints

Source: Regulatory Examination Guide

7

KEY QUESTIONS TO ASK YOURSELF

1. Can you articulate your organization's top 10 to 15 risks using a common scale as measured against earnings and capital?
2. Can the organization articulate the risks (type/amount) being leveraged as well as the limits for which it can support?
3. Does your program measure risk in real dollar terms against capital and earnings?
4. Does your program measure risk prospectively?
5. Does your program show the risk interdependencies and proactive risk influencers (KRI/KPI)?

8

KEY QUESTIONS TO ASK YOURSELF

6. Does it facilitate setting and understanding risk-tolerance levels?
7. Does it provide clarity for risk discussions and decisions between operations, management and the board of directors?
8. Does it facilitate open communication organization-wide regarding risk and decision making from strategy inception to operational execution?
9. Does the process provide targeted and actionable intelligence for business leaders?
10. What is your **confidence level** that processes are in place to effectively manage the vast array of risks across the organization?

9

WHAT IS RISK?

The possibility of an event occurring that will have a negative impact on the achievement of objectives.

Do you know your institution's objectives?

Risk is measured in terms of impact and likelihood.

The Institute of Internal Auditors (IIA)

10

WHAT IS RISK?

- **Known knowns** (cash over/shorts, credit losses, etc.)
- **Known unknowns** (data breach, fraud, etc.)
- **Unknown unknowns** (litigation, vendor failure, process breakdowns, etc.)

11

RISK TYPES

- Risk Categories:
 - Strategic
 - Reputation
 - Credit
 - Interest Rate
 - Liquidity
 - Transaction
 - Compliance
- Strategic
- Financial
- Operational

12

REWARDED VS. UNREWARDED RISKS

- **Rewarded Risks (Opportunities to take risk)**
 - Risks that are expected to bring some benefit if properly managed
 - Interest Rate Risk
 - Credit Risk
 - Liquidity Risk
 - Strategic Risks
- **Unrewarded Risks**
 - Those for which there is only a downside
 - Transaction Risk
 - Compliance Risks
 - Reputation Risk
 - Financial Reporting (Accounting) Risk

13

REGULATORY VIEW

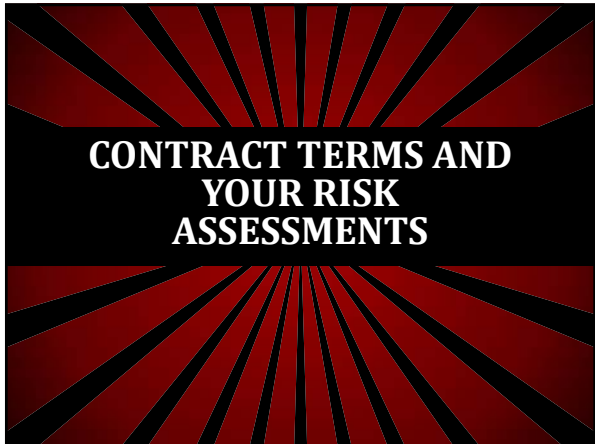
- **Comprehensive properly scaled risk management is a necessity**
- **Risk appetite and level of sophistication defines proper approach**
- **Avoidance is inefficient but a potential alternative for some institutions**
- **Not all risks arise from financial assets**
 - Cyber, product offerings, regulatory/criminal

14

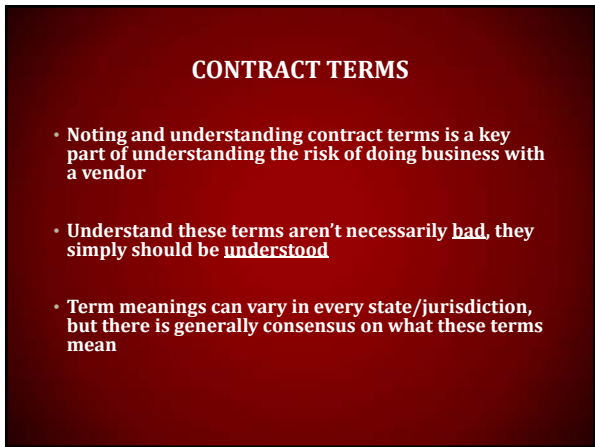
SUPERVISORY FOCUS ON RISK MANAGEMENT

- **Management commitment and oversight**
- **Well defined and integrated policies and procedures**
 - Clearly defined risk appetite
 - Clear understanding of the key risks and risk dynamics
 - Effective mitigation triggers and options
 - Effective risk reporting and monitoring
- **Appropriate information and decision support systems**
- **Effective internal controls**

15



16



17



18

FEEES

- Sounds easy, but fee disputes are the top reasons for litigation
- On a project, for example, do you understand what are cost estimates? What will be the charges for overruns?
- Be wary of fees not covered in the contract; proving fees are “unconscionable” in court is difficult

19

SECURITY

- GLBA extends to vendors by law if the vendor meets the definition of service provider. A service provider is defined as:
 - Any party that is permitted access to a financial institution's customer information through the provision of services directly to the institution

20

SECURITY

- “Reasonable” and “Commercially Reasonable” security are reasonably clear. Plaintiffs can use regulatory guidance, other cases, and other promises in the contract
- Commercially Reasonable is slightly lower than “best efforts” standards; what is prudent for similarly situated businesses

21

SECURITY

- You can try to negotiate requirements for minimum security (encryption, etc.)
- Implement a means to monitor the other sides' compliance
- Not all vendors will negotiate this language

22

WARRANTY AND REMEDIES

- Warranty is a guarantee of the quality of the services or products delivered
- Most of the time you will have limited or no warranties
- "As is" means in many cases you have no remedy once a product or service is delivered (no breach of contract)

23

WARRANTY AND REMEDIES

- "Professional" and/or "workmanlike" means work will be performed with reasonable care, skill and diligence
- Breach of this warranty may make the breaching party liable for all foreseeable damages
- Example: An accounting firm with an incorrect inventory balance causing an error in the calculation of cost of goods sold and, therefore, an error in the calculation of gross profit and net income

24

WARRANTY AND REMEDIES

- Your remedies are what happens if a warranty or the contract is breached
- Most companies will limit their liability; will your insurance also provide coverage?
- Also determine whether you will go to arbitration and who bears costs and fees

25

INDEMNIFICATION

- Indemnification means one party agrees to pay losses incurred by another to a third party
- You purchase a service, and that service is provided to your members. Members sue you, will the vendor providing the service defend you?

26

ASSIGNMENT

- Assignment is the right of a party to allow another to take over the rights and obligations in the contract
- If you have a vendor critical to your operations, you need to understand when and how a new vendor can take over these services

27

ASSIGNMENT

- Consent “shall not be unreasonably withheld” clause
- Difficult to deny assignment with this clause except if services are going to a competitor, or by transferring essential terms are going to change

28

TERM (AND TERMINATION)

- You need to know how long the contract is for, when it terminates, and if it renews
- If the agreement renews, when can you cancel the contract?
- Is the contract “no fault” for termination or will there be termination fees and other costs? (Also note if the vendor can walk away)

29

JURISDICTION (AND VENUE)

- Jurisdiction means which state law will apply, while venue is what court system will hear any cases
- Important to understand if there is dispute
- Most vendors will not negotiate jurisdiction; but having jurisdiction in the contract is better than none (lawyers can argue what law applies forever)

30

RECAP

- What are you paying for? What has the vendor guaranteed about the products or services?
- What has the vendor agreed to regarding security? Will you be indemnified for breach?
- Can the vendor walk away from the agreement, either through assignment or through termination/non-renewal?
- How will you wind down the relationship? What is your exit strategy?
- Which law applies? Will you have arbitration or file suit in a different jurisdiction?

31

**UNDERSTANDING AUDIT
REQUIREMENTS AND
MERGER CONSIDERATIONS**

32

AUDIT

- It is an **INDEPENDENT** testing of the BSA program
- Completed annually with an adequate scope
 - The BSA/AML Manual lays out details
- Can be conducted by an inside or outside auditor who is **INDEPENDENT** of the BSA process
- Results provided to the Board or their designated committee
- Results and work papers are available to the examiner

33

MINIMUM REQUIREMENTS

- Evaluation of the overall adequacy and effectiveness of the BSA program
- Review of the risk assessment
- Risk based transaction testing
- Evaluation of management's tracking and problem resolution
- Staff training
- Suspicious activity monitoring
- Process review, incl. SARs (Yes, they can SEE them)
- MIS integrity and accuracy

34

BEST PRACTICES

- Set expectations with auditor prior to beginning... if there is something you want to get out of the audit bring it up now
- Review risk assessment with Auditor as it forms the basis for the scope... if there is going to be a disagreement this is the time to hash it out
- Stick to regulations and avoid agreeing to best practice..... creates long term expense
- Review the checklist and determine if it comports to the FFIEC examiner guidelines... avoid scope creep

35

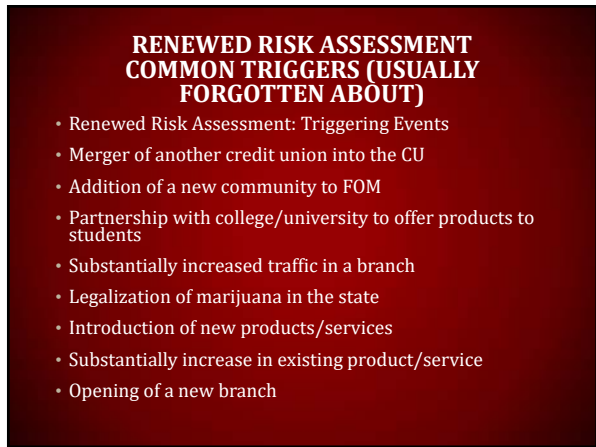
BEST PRACTICES

- Be available for questions and always have an end of day wrap up
- Ask what period is being used for the testing of CTR's and SAR's.
 - Too large...too narrow?
- Always have the exit interview prior to the auditor leaving. Discuss the findings rationally and make sure the expectation is that nothing outside of what was discussed during the exit interview will be in the report
 - Avoid the gotcha's
- Finally, your audit is what examiners will be basing their review upon. If you agreed to a recommendation, act upon it... if you disagreed than build and document your argument.

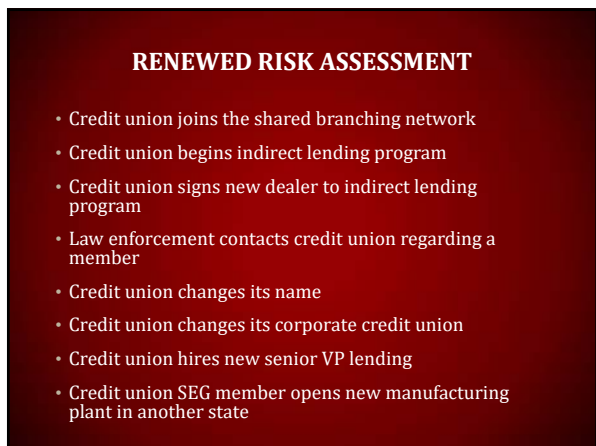
36



37



38



39

WHY CREDIT UNIONS CHOOSE TO MERGE?

- CEO retirement
- Board fatigue
- Financial hardships
- Regulatory burdens
- Regulatory pressure
- FOM issues
- Need access to products and services
- Strategic growth opportunities

40

LET'S DEFINE OUR TERMS

- Continuing Credit Union
 - Acquires the assets of the merging partner
- Merged Credit Union
 - Becomes part of the continuing credit union

41

THE GOOD WITH THE BAD

- In a merger, the continuing credit union assumes all of the liabilities of the merged credit union (unless you do a Purchase and Assumption).

42

IDENTIFICATION OF MERGER POSSIBILITIES

- Asset Size
- Market Area
- Field of Membership
- Financial Health & Capital
- Safety and Soundness
- Compliance
 - BSA

43

INVESTIGATION OF POTENTIAL PARTNERS

- Run the Numbers
 - What will the combined credit union look like
 - Depending on size - use third party (no endorsements)
- Determine Interest
- If Interested, NDA
 - Simple to complex - with no shopping or standstill

44

DUE DILIGENCE

- Mergers are Full of Surprises
- Plan the Investigation
 - Involve
 - Operations
 - Branch
 - HR
 - Legal
 - Technology
 - Compliance
 - BSA

45

DUE DILIGENCE II

- Conducting the Investigation
 - Key Compliance Issues
 - BSA
 - Review all third party vendor contracts
 - Complete Loan Review
 - Indirect Lending
 - Business Purpose and Business Lending
 - Real Estate
 - Collections
 - HR identifies key players to retain/be retained

46

NEGOTIATION OF THE TERMS

- NCUA Form
- Real Merger Agreement
 - When Merger will Happen
 - What Happens to Product & Services
 - What Happens to Personnel
 - What Happens to CEO/CFO
 - Who Makes Public / Member Announcements
 - Those Pesky Vendor Contracts/Agreements

47

INTEGRATION OF THE ENTITIES

- Accounting systems
- Staff functions and evaluations
- Policies
- Procedures
- Training

48

BSA MERGER DUE DILIGENCE

- Are you at the table to begin with the merger team?
- Understand the implications of taking on BSA violations or liability
- Start with an understanding of the merging credit union's risk appetite and culture
- Quality of their audits and examinations
- Examination findings, FinCEN correspondence and law enforcement entanglements
- Evaluation of their risk assessment and review of corresponding policies – especially areas outside your operations
- Sample filings with FinCEN and evaluate process in place for 314a scans and OFAC scans

49

BSA MERGER DUE DILIGENCE

- Evaluate their products and services and business lines that elevate risk
- Evaluate field of membership where additional risk could be present
- Evaluate the geography of the credit union
- Combine the two credit unions risk assessments and determine if there remains elevated residual risk
- Evaluate systems in place that uncover high risk accounts
- Was their risk assessment based upon reliable data?

50

QUESTIONS?

51



52
