Vendor Due Diligence Best Practices

ACUIA Webinar

PBMares SM
CPAs and Consultants

May 17, 2023 | www.pbmares.com

About PBMares, LLP

PBMares℠
CPAs and Consultants

Mid-Atlantic top 100 CPA and consulting firm

Offering

- Audit and Assurance
- Co-Sourced and Outsourced Internal Audit
- Cybersecurity
- Quality Assurance Review
- Business Advisory
- Risk Advisory
- Regulatory Compliance
- Transaction Advisory

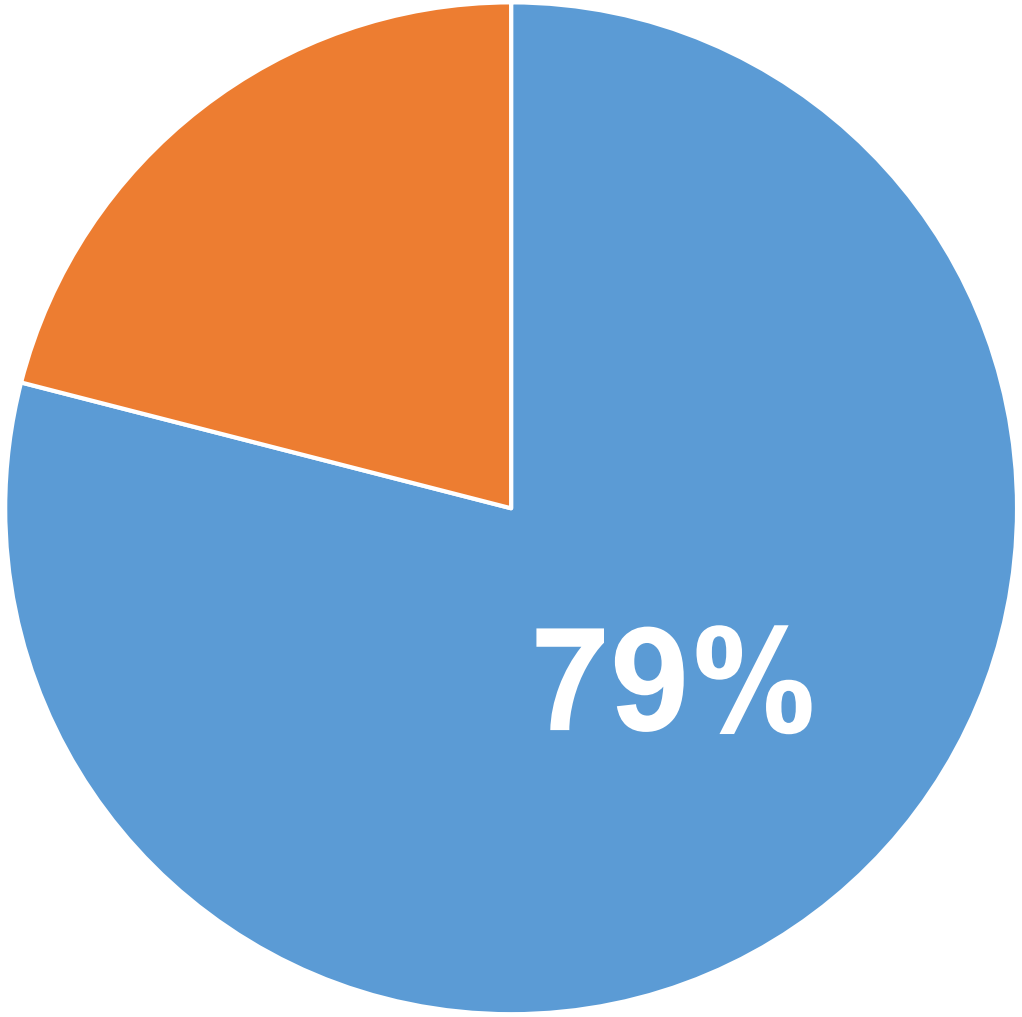
Ice Breaker

PBMares SM
CPAs and Consultants

Where is everyone going on vacation this summer? Answer in the chat!

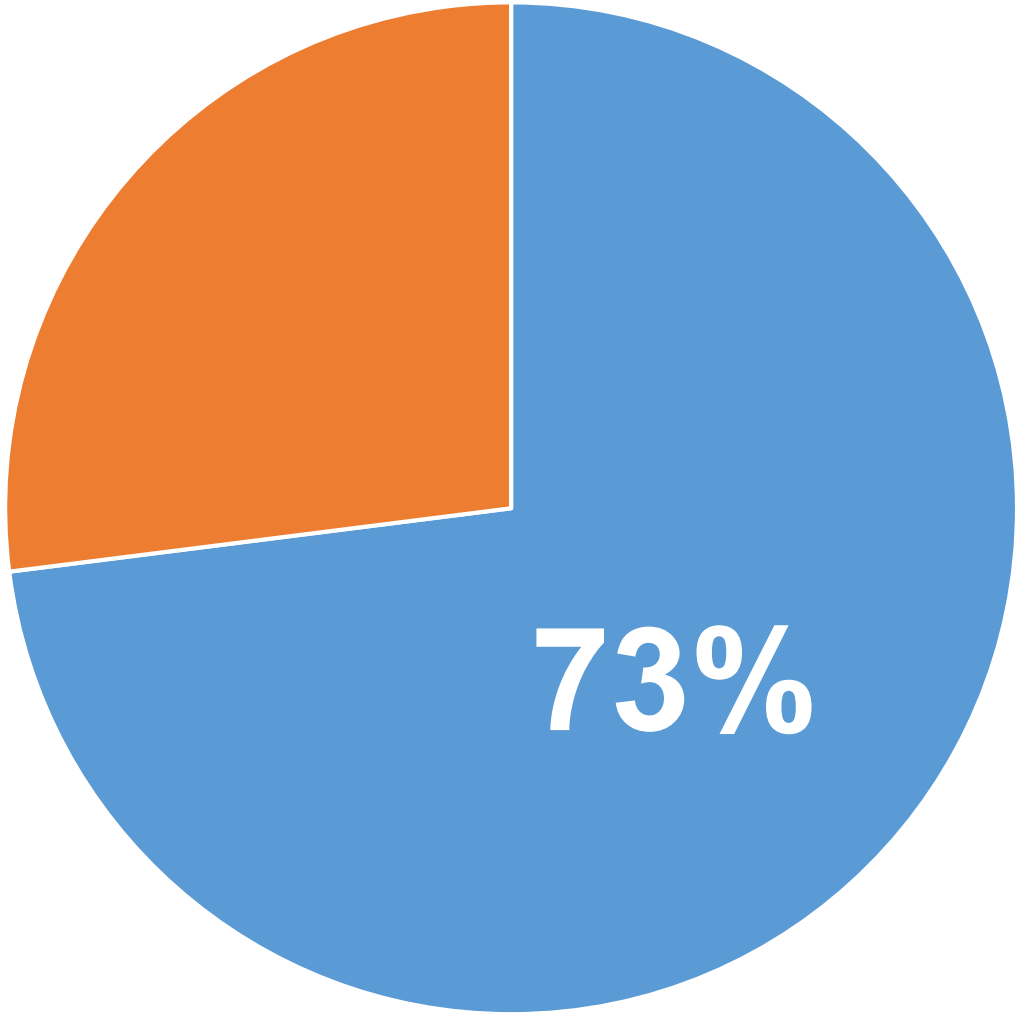
Third Party Vendor Risk

79% of businesses are adopting technologies faster than they can address related security risk



Third Party Vendor Risk

"73% of organizations have experienced at least one significant disruption caused by a third party vendor"



Data is the New Oil

PBMares SM
CPAs and Consultants

PBMares SM
CPAs and Consultants

Polling Question

Why is evaluating the Vendor Due Diligence becoming more prevalent?

PBMares SM
CPAs and Consultants

- ✔ No one remembers the name of the third-party causing the disruption in operations
- ✔ The fault and possible reputation damage lies with the organization itself
- ✔ Reputational damage is difficult to anticipate and recover
- ✔ Significant data breaches involving third parties could cause a material loss

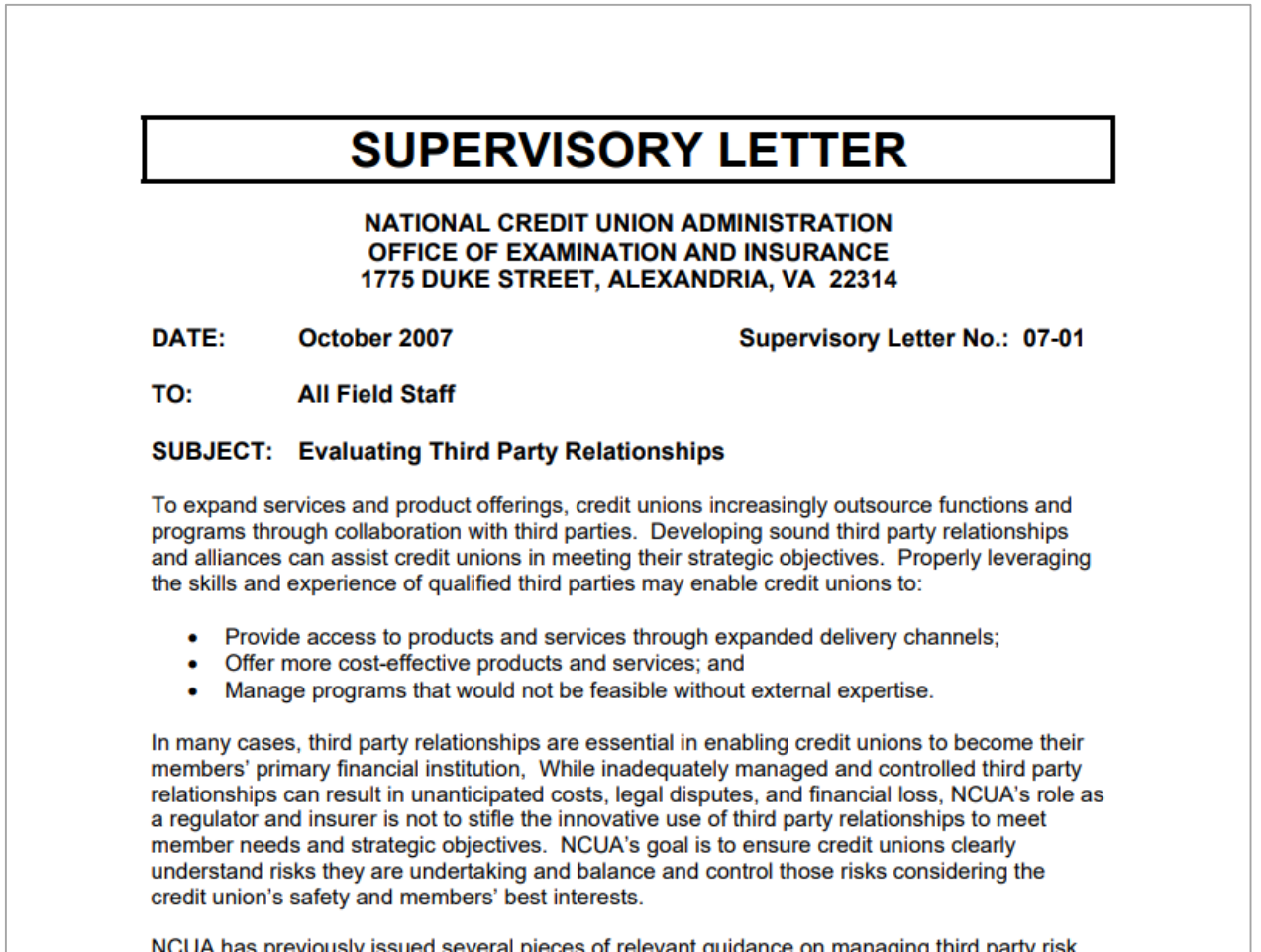
This makes robust third-party risk assessment, due diligence, and monitoring even more critical.

Regulations

- ✔ NCUA letter
  SL No. 07-01 / October 2007

- ✔ VDD falls into multiple areas of the NCUA 2023 Supervisory Priorities
  - Information Security (Cybersecurity)
  - Consumer Financial Protection

- ✔ FFIEC Handbook – Outsourcing Technology Services Booklet



SUPERVISORY LETTER

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF EXAMINATION AND INSURANCE
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: **October 2007** **Supervisory Letter No.: 07-01**

TO: **All Field Staff**

SUBJECT: **Evaluating Third Party Relationships**

To expand services and product offerings, credit unions increasingly outsource functions and programs through collaboration with third parties. Developing sound third party relationships and alliances can assist credit unions in meeting their strategic objectives. Properly leveraging the skills and experience of qualified third parties may enable credit unions to:

- Provide access to products and services through expanded delivery channels;
- Offer more cost-effective products and services; and
- Manage programs that would not be feasible without external expertise.

In many cases, third party relationships are essential in enabling credit unions to become their members' primary financial institution, While inadequately managed and controlled third party relationships can result in unanticipated costs, legal disputes, and financial loss, NCUA's role as a regulator and insurer is not to stifle the innovative use of third party relationships to meet member needs and strategic objectives. NCUA's goal is to ensure credit unions clearly understand risks they are undertaking and balance and control those risks considering the credit union's safety and members' best interests.

NCUA has previously issued several pieces of relevant guidance on managing third party risk

Risks to Consider When Evaluating VDD Program

- ✔ Strategic
- ✔ Reputation
- ✔ Transaction
- ✔ Credit
- ✔ Compliance
- ✔ Financial

Identifying Potential Vendor Risks

- Third-party dependency
- Compliance issues
- Quality control issues
- Reputation risk
- Contractual issues
- Communication breakdown
- Data breaches

PBMares SM
CPAs and Consultants

Polling Question

Benefits of a Strong Due Diligence Program

- ✔ Risk Management
- ✔ Regulatory Compliance
- ✔ Cost Savings
- ✔ Reputation Management
- ✔ Improved Vendor Relationships

Outsourcing a VDD Program?

The FFIEC has their own examination procedures covering factors to consider such as:

- Criticality
- Cost
- Compliance
- Data/Information Sharing

Implementing a Vendor Due Diligence Management Program

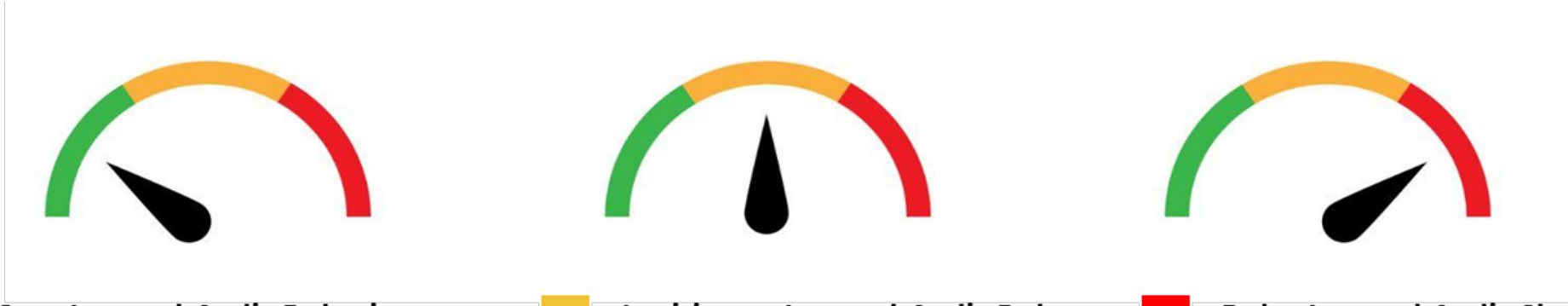
PBMares SM
CPAs and Consultants

The 3 Components of 3rd Party Management

1. Risk Assessment and Planning
2. Effective Due Diligence
3. Risk Measurement, Monitoring, and Control

What if Internal Audit is Involved in Vendor Due Diligence?

PBMares SM
CPAs and Consultants



Core Internal Audit Roles in Regard to ERM

- Giving assurance on the risk management processes
- Giving assurance that risks are correctly evaluated
- Evaluating risk management processes
- Evaluating the reporting of key risks
- Reviewing the management of key risks

Legitimate Internal Audit Roles with Safeguards

- Facilitating identification and evaluation of risks
- Coaching management in responding to risks
- Coordinating ERM activities
- Consolidated reporting on risks
- Maintaining and developing the ERM framework
- Championing establishment of ERM
- Developing RM strategy for board approval

Roles Internal Audit Should NOT Undertake

- Setting the risk appetite
- Imposing risk management processes
- Management assurance on risks
- Taking decisions on risk responses
- Implementing risk responses on management's behalf
- Accountability for risk management

Conducting a Vendor Due Diligence Audit

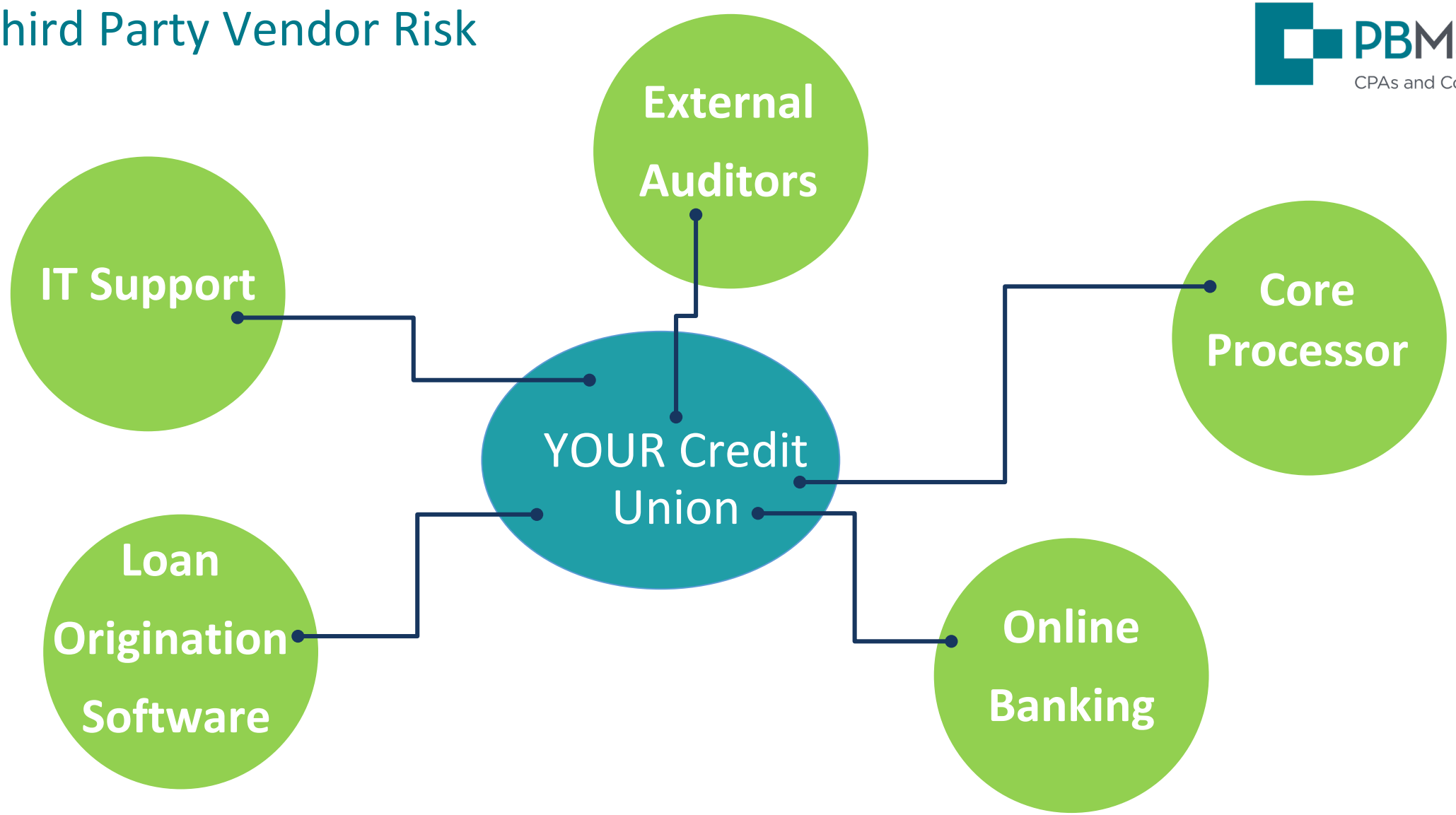
PBMares SM
CPAs and Consultants

- Review policies and procedures
- Inquire about the background of VDD program
- Develop an audit plan tailored to the VDD program

Auditing Vendor Due Diligence Policy/Procedures

- Record retention
- Master vendor list
- Risk Appetite of Credit Union
- Red flags and warning signs
- Criteria for selecting vendors
- Guidelines for review of vendors
- Holding all vendors a standard
- Avoiding vague/ambiguous terms

Third Party Vendor Risk



PBMares SM
CPAs and Consultants

Polling Question

Continually Monitoring Vendor Performance

PBMares SM
CPAs and Consultants

- Timing of review
- Documenting Complementary User Entity Controls (CUECs)
- Ensuring you have all SOC reports (SOC 1 vs SOC 2 and Type 1 vs Type 2)

Addressing Vendor Non-Compliance

- What is the plan if a vendor is not in compliance with the Credit Union's risk appetite but they are a critical vendor?

- Do you have contingencies for when:
  - You did not receive requested information
  - What documents are deal breakers?
  - Is corrective action needed?

Vendor Termination if “Sh*t hits the fan”

PBMares SM
CPAs and Consultants

- Do you have a termination clause in your contract?
- Is there penalties for lack of performance?
- What is the record retention clause after termination?

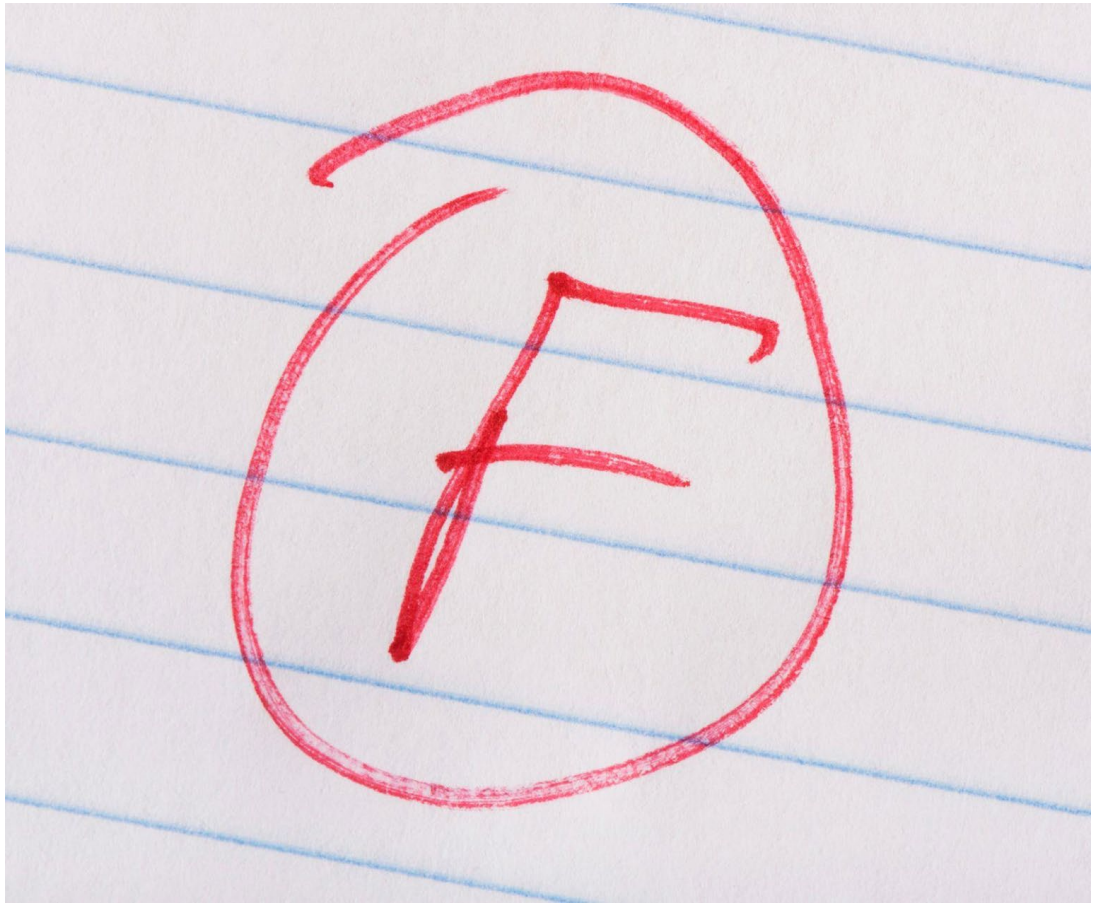
“Hoping for the best, prepared for the worst, and unsurprised by anything in between.”

Third Party Contracts Should Address:

- ✓ Scope of arrangement
- ✓ Responsibilities of all parties
- ✓ Performance standards and measures
- ✓ Frequency of reporting
- ✓ Penalties for lack of performance
- ✓ Access to financial and operating records
- ✓ Ownership of servicing rights
- ✓ Responsibility for payment
- ✓ Data security and member confidentiality
- ✓ Contingency planning
- ✓ Insurance
- ✓ Member complaints and member service
- ✓ Compliance with regulatory requirements (e.g. GLBA, Privacy, BSA, etc.)
- ✓ Dispute resolution
- ✓ Default, termination, and escape clauses

Common Audit Recommendations

- Risk assessment is not measurable or consistent
- Incomplete or inaccurate vendor information and insufficient follow-up
- Incomplete approved vendor listing
- Lack of standardization
- Inadequate ongoing monitoring
- Over reliance on third-party performing VDD
- Non-adherence to policy
- Failure to review and test CEUCs
- Vague or contradicting policy



In Conclusion

PBMares SM
CPAs and Consultants

- Third-party risk is rapidly growing and evolving
- VDD is an increasingly critical process
- Read your vendor contracts and then read them again
- Develop a standardized system for evaluating vendors
- Vendor non-compliance = credit union non-compliance
- It is the credit union's reputation on the line not your vendor's

Questions

PBMares SM
CPAs and Consultants

Contact

PBMares SM
CPAs and Consultants

William “JJ” Edmunds, Jr.
CPA, CIA, CISA, MSA
Risk Advisory Senior Manager

wedmunds@pbmares.com
804.977.5059

Stacy Moore, CPA
Risk Advisory Supervisor

slmoore@pbmares.com
240.499.2047

www.PBMares.com