# Crossroads of Risk

## CYBERSECURITY, COMPLIANCE and VENDOR MANAGEMENT

Presented by:
On: Tuesday, September 25, 2018





## What is the Risk?

# What is the Risk?

## Equifax Breach: Result of Vendor Security Issue

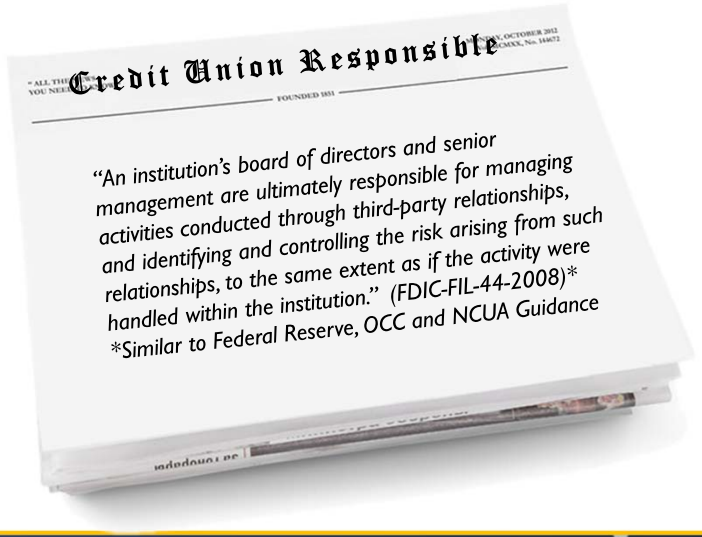
- **Credit reporting company Equifax said that an additional 2.5 million Americans may have been affected by a massive security breach this summer. That brings the total number of Americans whose data was exposed to 145.5 million people ...Oct 2, 2017**

**Forbes, January 17, 2014**





# Liability



# Enforcement Actions

- InTouch CU (Texas) (2017) – ransom ware at vendor led to data compromised. As a result change accounts and cards for all effected accounts and data monitoring for thousands of members
- Security Breach Community Bank - 3rd party core processor had a security breach that resulted in fraudulent debit card charges to deposit account. credit union had to reimburse members even thought the third party was at fault.





# Regulatory Requirements Background

**57**

Number of years service providers have been a regulatory issue

Bank Service Company Act of 1961

Outsourcing now includes services and solutions beyond IT

(FIL-20-2008)

Vendors are involved in most every product or service

FI is no longer in complete control of non-public member data

Increased reliance on vendors to safeguard data

# Cybersecurity

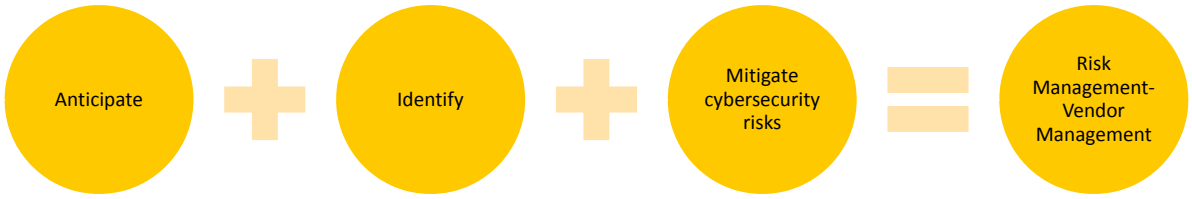




# Cybersecurity - What is Required?

- NCUA recognizes the importance of cybersecurity and using the web safely and securely.
- NCUA expects credit unions to have the appropriate procedures in place to anticipate, identify, and mitigate cybersecurity risks.
  - Specific expectations can be found in the body and appendices of ***Part 748 of NCUA regulations*** as well as the FFIEC IT Examination Handbooks.
- FFIEC's cybersecurity assessment tool is provided to help credit unions assess their level of preparedness
  - NCUA examiners will use the tool as a guide for assessing cybersecurity risks in credit unions.
  - Credit unions may choose whatever approach they feel appropriate to conduct their individual assessments, but the assessment tool would still be a useful guide.

# Cybersecurity –What is Required?




NCUA Supervisory Letter 07-CU-13, Part 748, FFIEC Handbook




# NCUA Supervisory Letter No. 07-CU-13

## Vendor Management

- Officials must carefully consider the potential risks these relationships may present and how to manage them.
- As credit unions seek to manage risk, they should carefully consider the correlation between their level of control over business functions and the potential for compounding risks.
- Credit unions maintaining complete control over all functions may be operationally or financially inefficient. Credit unions outsourcing functions without the appropriate level of due diligence and oversight may be taking on undue risk.
- Ultimately, credit unions are responsible for safeguarding member assets and ensuring sound operations irrespective of whether or not a third party is involved

# Part 748 – Appendix A

- **Information Security Program**. A comprehensive written information security program includes administrative, technical, and physical safeguards appropriate to the size and complexity of the credit union and the nature and scope of its activities…
- **Objectives.** A credit union's information security program should be designed to:
  - ensure the security and confidentiality of member information;
  - protect against any anticipated threats or hazards to the security or integrity of such information;
  - protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member;
  - and ensure the proper disposal of member information and consumer information.
  - Protecting confidentiality includes honoring members' requests to opt out of disclosures to nonaffiliated third parties.




# Part 748 – Appendix A

- The Information Security Policy should
  - Involve the Board of Directors
  - Assess Risk
  - Manage and Control Risk
  - Oversee Service Provider Arrangements
  - Adjust the Program
  - Report to the Board

# Part 748 – Appendix A

**Oversee Service Provider Arrangements**. Each credit union should:

- Exercise appropriate due diligence in selecting its service providers;
- Require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines; and
- Where indicated by the credit union's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2.
  - As part of this monitoring, a credit union should review audits, summaries of test results, or other equivalent evaluations of its service providers.




# Bottom Line

GLBA- Gramm–Leach–Bliley Act

- Governs the collection, disclosure, and protection of consumers personal information and personally identifiable information by financial institutions (GLBA Info/ NPPI). It requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.
- Non-public personal information (“NPPI”) is any personal information that cannot be found in public sources. Publicly available information would be details available from federal, state, or local government records; widely distributed media (such as telephone directories or newspapers); or information disclosed to the public as required by federal, state, or local law. NPI is usually obtained directly from the individual. It includes such details as the person’s date of birth, social security number, financial account numbers and balances, sources and amounts of income, credit card numbers, information obtained about visitors to your Internet web site, and sometimes could include home addresses and telephone numbers.

# Risk Assessment

Monitor, Assess and begin again

Residual Risk

Due Diligence
Assess Controls

Identifying Risks

Typical Areas of Risk: Strategic, Reputation, Operational, Transaction, Credit, Compliance, Other

Benefits of Outsourcing

Business Strategy
Outsourcing Consistent with Business Strategy

Gather Data from Internal Resources

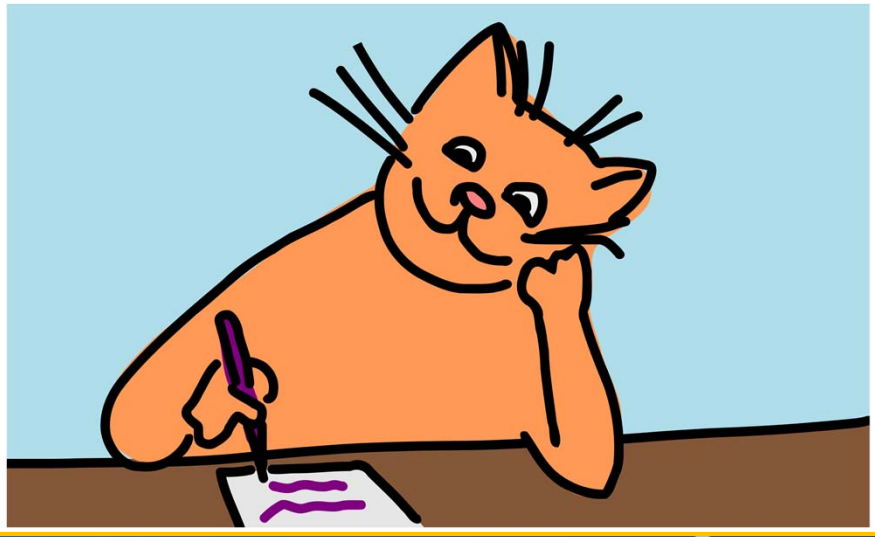
IT, Operations, Compliance, Legal, Finance

What is my Inherent Risk?





# The CAT – The New King of Assessments



## CAT

### Cybersecurity Assessment Tool (CAT)

- Released in the summer of 2105 by the FFIEC
- It provides a structured methodology for credit unions to manage information security and protect member information more effectively.
- Provides credit unions with a repeatable and measurable process to inform management of their risks (Inherent Risk Profile) and cybersecurity preparedness in relation to that risk (Cybersecurity Maturity).
- It is designed to enhance Cybersecurity oversight and management capabilities, and to identify gaps in a credit union's risk management practices.
- 10 percent of these questions address external dependencies (aka vendors)
  - Example: "Contracts establish responsibilities for responding to security incidents?"





## CAT

### Cybersecurity Assessment Tool (CAT)

- If the level of preparedness is not adequate, the credit union may take action either to reduce the level of risk or to increase the levels of maturity (a "target" state).


- The CAT is meant to be used on an enterprise-wide level periodically or as technology changes.
- The CAT is mapped to both the *FFIEC Information Technology Examination Handbook (FFIEC IT Handbook),* as well as the *National Institute of Standards and Technology (NIST) Cybersecurity Framework*

Copyright 2017 Ncontracts, LLC. All rights reserved.

Ncontracts

## CAT

In May 2017, the FFIEC updated the CAT to include updated references to the *FFIEC IT Handbook* and update some responses in the Cybersecurity Maturity section.

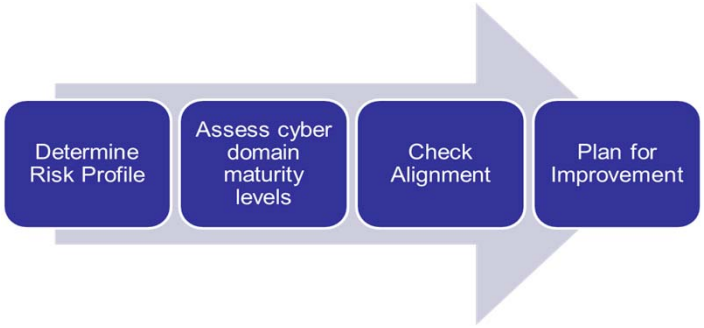
- The mappings in Appendix A were updated to reflect recent changes to the FFIEC IT Handbook.
- In the Cybersecurity Maturity section, rather than the binary “yes” or “no” responses in the previous version, credit unions may now select between, “yes,” “no” and “yes – with compensating controls”.
  - Additionally, a combination of “yes” or “yes- with compensating controls” being selected in any one domain level will qualify as meeting that level of maturity. Like the previous version, if “no” is indicated anywhere within a particular level, that level will not be considered met.





## CAT

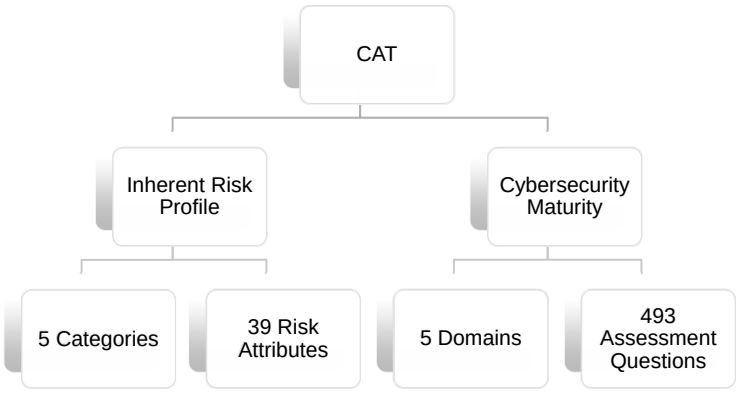
- How does the process work?




Copyright 2017 Ncontracts, LLC. All rights reserved.

ncontracts

## CAT








## CAT – Let's Take a Breather

- Remember - The CAT is meant to be used on an enterprise-wide level periodically or as technology changes.
  - When we implement the CAT, think enterprise-wide
  - You will need the input and help of many people.
  - Beware of the CAT hog!

  - Most importantly, you will need to start from the top.
  - **A detailed, effective cybersecurity assessment is dependent upon executive management's oversight and support.**

## CAT – Inherent Risk

- The Inherent Risk Profile identifies activities, services, and products organized in categories with a brief description of what is included in each category. The credit union selects the most appropriate risk level for each one.
- Following this part of the exercise, the credit union will then tally up its results to determine its risk profile.
  - For instance, a very small credit union will likely be in the least-moderate inherent risk categories. Larger credit unions will likely be in the two higher categories of risk.

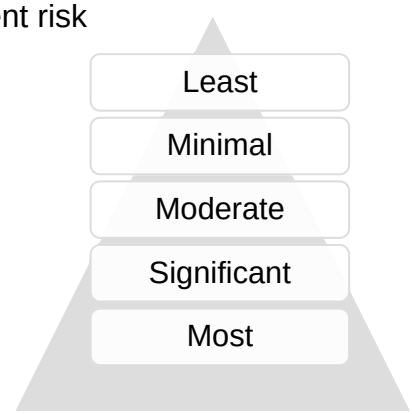




## CAT – Inherent Risk

## CAT – Inherent Risk

- 5 levels of inherent risk








## CAT - Inherent Risk

- Least Risk: Limited use of technology; zero connections; products and services are limited; and a small footprint and few employees.
- Minimal Risk: Limited variety of less risky products/services; mission-critical systems are outsourced; use established technologies; and maintain few types of connections with limited complexity.
- Moderate Risk: Somewhat complex technology in terms of volume and sophistication; may outsource mission-critical systems; have a greater variety of products and services offered through diverse channels.
- Significant Risk: Complex technology; offer high-risk products/services that may include emerging technologies; may host significant number of applications internally; have a substantial number of connections to customers and third parties; offer a variety of payments directly or through a third party; and may have significant volume.
- Most Risk: Extremely complex technologies to deliver a myriad of products and services which may be at highest level of risk, including being offered to other organizations; new and emerging technologies are used across multiple delivery channels; outsource some mission critical systems of applications but most are hosted internally; and maintain a large number of connections.

## CAT - Inherent Risk

| Category: External | Risk Levels | | | | |
|---|---|---|---|---|---|
| | Least | Minimal | Moderate | Significant | Most |
| Attempted cyber attacks | No attempted attacks or reconnaissance. | Few attempts monthly (<100); may have had generic phishing campaigns by employees and customers. | Several attempts monthly (101-500); phishing campaigns targeting employees or customers at the institution or third parties supporting critical activities; may have experienced an attempted Distributed Denial of Service (DDoS) attack within the last year. | Significant number of attempts monthly (501-100,000); spear phishing campaigns targeting high net worth customers and employees at the institution or third parties supporting critical activities; Institution specifically is named in threat reports; may have experienced multiple DDoS attacks within the last year. | Substantial number of attempts monthly (> 100,000); persistent attempts to attack senior management and/or network administrators; frequently targeted for DDoS attacks. |





## CAT - Inherent Risk

- After reviewing each category and the various statements, the institutions will tally the risk columns. The column with the most responses will result in the Inherent Risk Profile.

## CAT – Maturity Level

Credit unions will next determine their cybersecurity maturity level.

- Five domains (or sections) and the assessment factors and components identified for each domain.
- Under each component there are declarative statements describing an activity that supports the assessment factor at that level of maturity.
  - In order to be considered at a particular maturity level, all declarative statements for that level must be selected.
  - For instance, to be considered at the Baseline level for Domain 1, Governance, the credit union must be able to affirmatively respond to all declarative statements within that level. If the institution moves on to the next level, Evolving, and can only answer three of four declarative statements affirmatively, it does not meet the Evolving level.



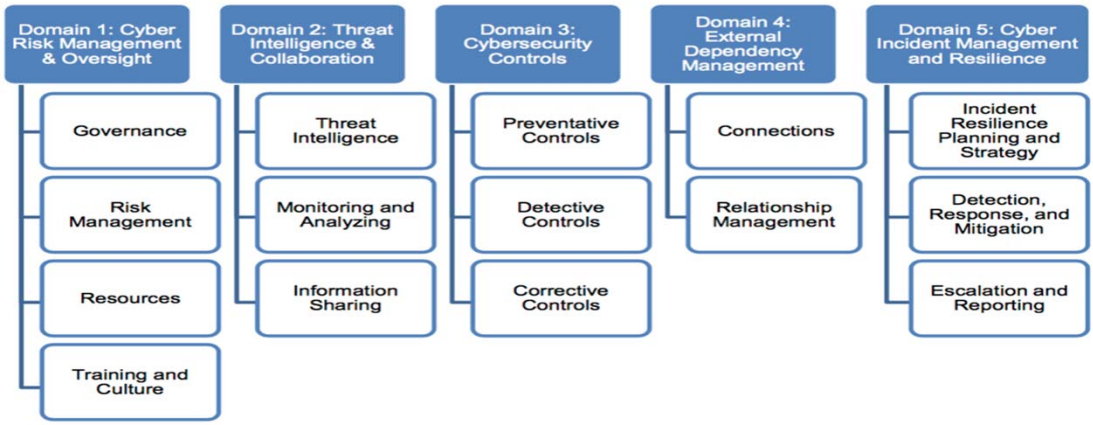


## CAT – Maturity Level


Copyright 2017 Ncontracts, LLC. All rights reserved.

ncontracts

## CAT – Cyber Maturity






ncontracts

## CAT – Cyber Maturity

**Domain 1: Cyber Risk Management and Oversight**
Addresses the Board of Directors' oversight and management's development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.

**Domain 2**: **Threat Intelligence and Collaboration**
Includes processes to effectively discover, analyze and understand cyber threats, with the capability to share information internally and with appropriate third parties.

**Domain 3: Cybersecurity Controls**
Includes the practices and processes used to protect assets, infrastructure and information by strengthening the institution's defensive posture through continuous, automated protection and monitoring.

**Domain 4: External Dependency Management**
Involves establishing and maintaining a comprehensive program to oversee and manage external connections and third party relationships with access to an institution's technology assets and info.

**Domain 5: Cyber Incident Management and Resilience**
Includes establishing and analyzing cyber events, prioritizing the institution's containment or mitigation and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber incident.



ncontracts

## CAT – Cyber Maturity

Minimum expectations required by law and regulation, or recommended in supervisory guidance. Management has reviewed the evaluated guidance

- Baseline

Documented procedures and policies. Risk driven objectives are in place. Cybersecurity is formally assigned

- Evolving

Detailed, formal processes. Controls are validated and consistent. Risk management practices and analysis are integrated into business strategies . Accountability for cybersecurity is formally assigned and broadened beyond protection of info, and involves information systems.

- Intermediate

Practices and analytics that are integrated across lines of businesses. Majority of risk management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline business is formally assigned

- Advanced

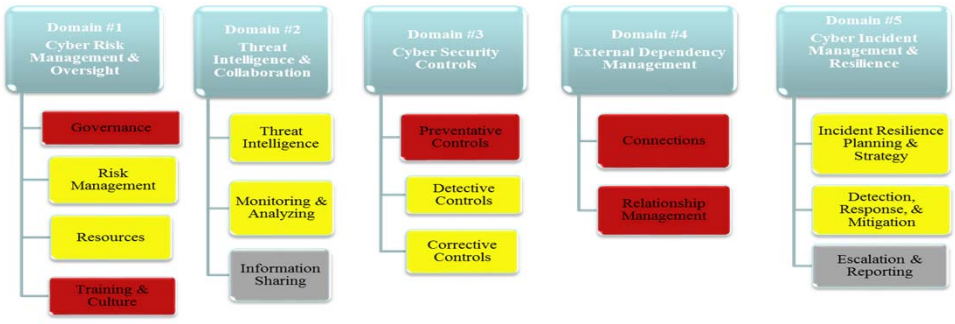
Driving innovation in people, processes and technology for the organization and industry to manage cyber risk. May involve developing new controls or tools

- Innovative





## CAT – Cyber Maturity



# The ACET

## Automated Cybersecurity Examination Tool

- A new tool developed in 2017 by the NCUA to help examiners assess a credit union's level of cybersecurity preparedness.
  - It provides the NCUA with a repeatable, measurable and transparent process that improves and standardizes its supervision related to cybersecurity in all federally insured credit unions.
- It mirrors the FFIEC's CAT developed for voluntary use by banks and credit unions.
- Like the CAT, the ACET consists of two parts: the Inherent Risk Profile and the Cybersecurity Maturity level.
  - The Inherent Risk Profile in the tool helps determine a credit union's exposure to risk by identifying the type, volume, and complexity of the institution's operations.
  - The Cybersecurity Maturity portion of the tool is designed to help us measure a credit union's level of risk and corresponding controls. The levels range from baseline to innovative.




# The ACET

- The ACET incorporates appropriate cybersecurity standards and practices established for financial institutions.
  - The tool maps each of its declarative statements to these best practices found in the FFIEC's IT Examination Handbook, regulatory guidance, and leading industry standards like the National Institute of Standards and Technology's Cybersecurity Framework .
  - The tool also provides examiners a plain-language explanation and references for each of the declarative statements included in the assessment.
- In 2018, the NCUA will review credit unions with $1 billion or more in assets using the ACET.
  - The ACET will be refined to ensure it scales properly for smaller, less complex credit unions.
  - The ACET will be used over the next few years to benchmark the industry's preparedness levels.
  - These benchmarks will be used to start a dialog on how the credit union system's cybersecurity preparedness levels can be improved.
- Using the new ACET ensures the NCUA is consistent in its approach and can scale its expectations properly to the size, complexity and risk exposure of each credit union.
  - The tool will also provide valuable insights that will help the NCUA focus its supervision efforts on areas that are the most important for the credit union system.

# Cybersecurity and Vendors





# Classifying Vendors

What does ”risk assess my vendor” mean?

- Inherent Risk vs Residual Risk
- Which vendors for cyber?
- The CAT uses the term critical vendors and cites vendor management guidance in reference to vendors for external dependency questions.

# Which Vendors Need Reviews?

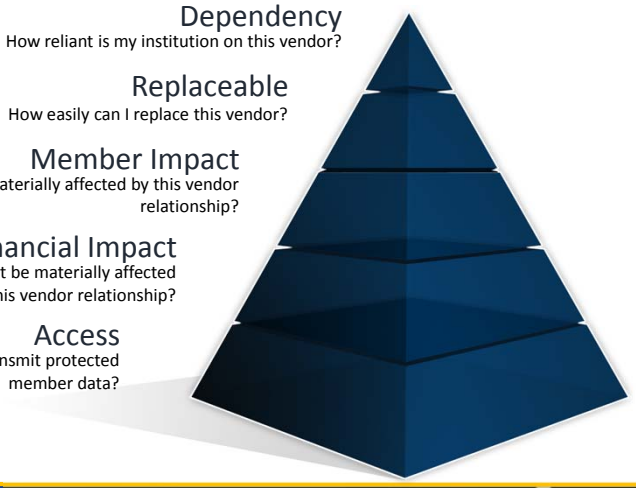
**Dependency**
How reliant is my institution on this vendor?

**Replaceable**
How easily can I replace this vendor?

**Member Impact**
Would my member be materially affected by this vendor relationship?

**Financial Impact**
Would the P&L or balance sheet be materially affected by this vendor relationship?

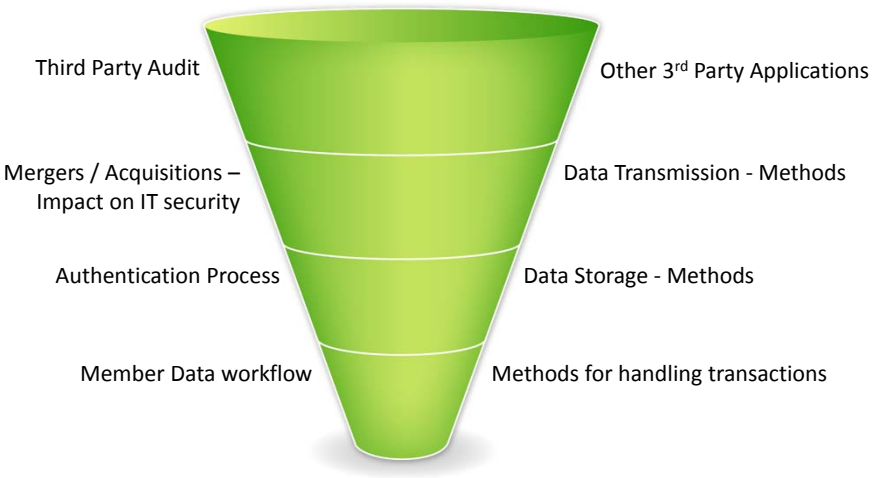
**Access**
Does the vendor store and transmit protected member data?







# Due Diligence – Process Review



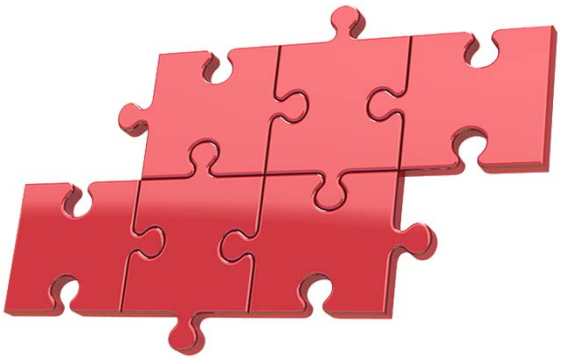
# Documents to Gather


- Financials (3rd Party Review)
- SSAE 18
- Disaster Recovery Plans/Tests
- Incident Response Plans/Tests
- Government Reports on Vendor
- Info. Security Policy
  - Security Awareness Training
  - Security Plans
- Cybersecurity Plans

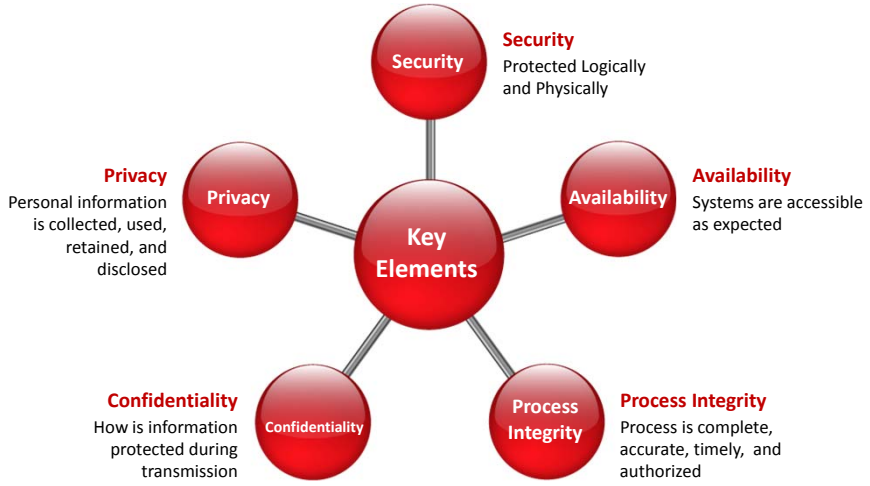



# SSAE / SOC 18 Reports

- Scope
  – Defines work
- Exceptions
  – How corrected
- User Controls
  – Products utilized
- Identify Strengths



# SSAE 18 / SOC – Key Elements








# Exceptions

- What happened?
- Is my data compromised?
- Is my access compromised?
- What mitigates the finding?
- Does my institution need to follow up?
- Does my gap letter address the issue?

# Meeting GLBA Standards

- Access controls over member information systems
- Access restrictions at physical locations
- Controls to ensure the security/encryption of electronic member information and measures to ensure proper disposal
- Controls over system modifications
- Dual control procedures, segregation of duties, background checks for employees
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems
- Response programs when a financial institution suspects or detects unauthorized access
- Measures to protect against destruction, loss or damage of member information due to environmental hazards
- Staff training on information security
- Regular Testing of key controls, systems, and procedures for the information security program
- Oversight of service provider arrangements

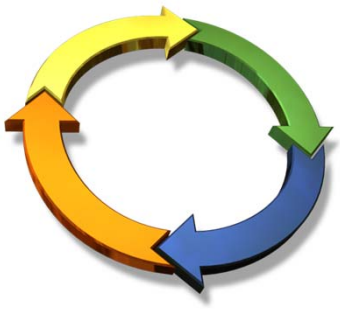



# SSAE 18 Key Considerations

- What was tested?
- Why was it tested?
- Context of products used by institution?
- Documentation is the key – more than a questionnaire or checklist.

# Ongoing Monitoring for Cyber and VM

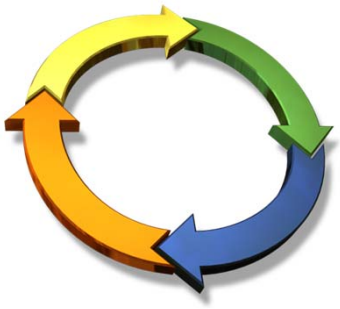
- Annual Review for Risk Assessments of Designated Vendors
  - SSAE 18s
  - Disaster Recovery Plans / Tests
  - Incident Response Plans / Tests
  - Financials
  - Summary of Findings and Evaluation






# Ongoing Monitoring for Cyber and VM

- Monitoring is More than Annual Assessment
  - Litigation
  - Vendor Sold / Acquired
  - Data Breach
  - Regulatory Issues and Compliance
  - News
  - SLAs
  - Compliance with Contract Terms
  - Insurance



# Leveraging the Contract Risk – Key Issues

1. Scope
2. Security Incidents
3. Retaining Information – IT Security
4. Business Resumption – Contingency Planning – Resilience
5. Compliance with Laws
6. Right to Audit
7. Confidentiality
8. Indemnity
9. Insurance
10. Subcontracting - Assignment





# Scope

| | |
|---|---|
| **Meaning:** | What does the vendor provide in service, support and software? |
| **Issues to Look for:** | Could someone who has never seen the solution (a regulator) understand the purpose of the agreement by only reading the agreement? |
| **Mitigation:** | Need details to describe why you have this service, software, and or support. |

# Security Incidents

| | |
|---|---|
| **Meaning:** | How does the vendor handle security incidents? |
| **Issues to Look for:** | Preventative measures to prevent unauthorized access<br>Notice provisions for incidents<br>Plan for handling breaches |
| **Mitigation:** | Form details of what your organization will want and have predefined language drafted to add to agreements. |




# Retaining Information – IT Security

| | |
|---|---|
| **Meaning:** | Who owns the data? Where is it hosted? What levels of security are in place? Who tests the security? |
| **Issues to Look for:** | Ownership of the data is key. Should have provisions regarding IT security. If there is a dispute or issue, how does the credit union continue to deliver service to the member? |
| **Mitigation:** | Details of IT security and details that the credit union owns their data. |

# Business Resumption, BCP, Resilience

| | |
|---|---|
| **Meaning:** | The disaster recovery plan and test of the plan for the vendor. |
| **Issues to Look for:** | How often are they required by contract to test their plan? How fast can they be back up and running? |
| **Mitigation:** | Details should coincide with how critical the vendor is to the credit union. |




# Compliance with Laws

| | |
|---|---|
| **Meaning:** | Vendor must comply with particular statutes, be subject regulatory reviews, and provide data for compliance. |
| **Issues to Look for:** | Does your state have specific rules that require more? (CA and Mass. have additional privacy laws) |
| **Mitigation:** | Look for specific language that meets the criteria. |

# Right to Audit

| | |
|---|---|
| **Meaning:** | Right to review the internal operations of the vendor |
| **Issues to Look for:** | What level of notice is required? What is the credit union allowed to see? Who gets to perform the audit? |
| **Mitigation:** | Add provisions that require data to be shared to prove cybersecurity measures are in place |




# Confidentiality

| | |
|---|---|
| **Meaning:** | Do the parties have to keep information just between the parties to the contract. Typically, will include GLBA compliance language if client data is involved or could be involved. |
| **Issues to Look for:** | How do the provisions protect the credit union, not just the vendor. |
| **Mitigation:** | Use form language that is every agreement |

# Indemnity

| | |
|---|---|
| **Meaning:** | When one party will take the place of another in a legal claim. |
| **Issues to Look for:** | Does the credit union have to indemnify the vendor?<br>Are there instances where the vendor should be indemnifying the credit union? (Ex: ATM Patent Trolls or breaches of security from vendor) |
| **Mitigation:** | Specific language for indemnification that should include notice provision and who controls the defense of the claim. |




# Insurance

| | |
|---|---|
| **Meaning:** | Is the vendor required to maintain insurance? If so, what type? Does it fit the services being provided? |
| **Issues to Look for:** | E&O- Cybersecurity (sometimes a part of the E&O coverage)<br>D&O |
| **Mitigation:** | Should require adequate levels of insurance to cover liability or breach. Should require vendor to provide annual certificate of insurance. |

# Subcontracting - Assignment

| | |
|---|---|
| **Meaning:** | Can the vendor transfer their rights and responsibilities to a third party? |
| **Issues to Look for:** | If Agreement is silent, then it is assignable.<br>If critical vendor, may have additional vendors to review because of outsourcing |
| **Mitigation:** | Should require notice and consent of credit union prior to assignment. |




# Contact Information

888-370-5552 x7379

mitchell.klein@ncontracts.com

www.ncontracts.com