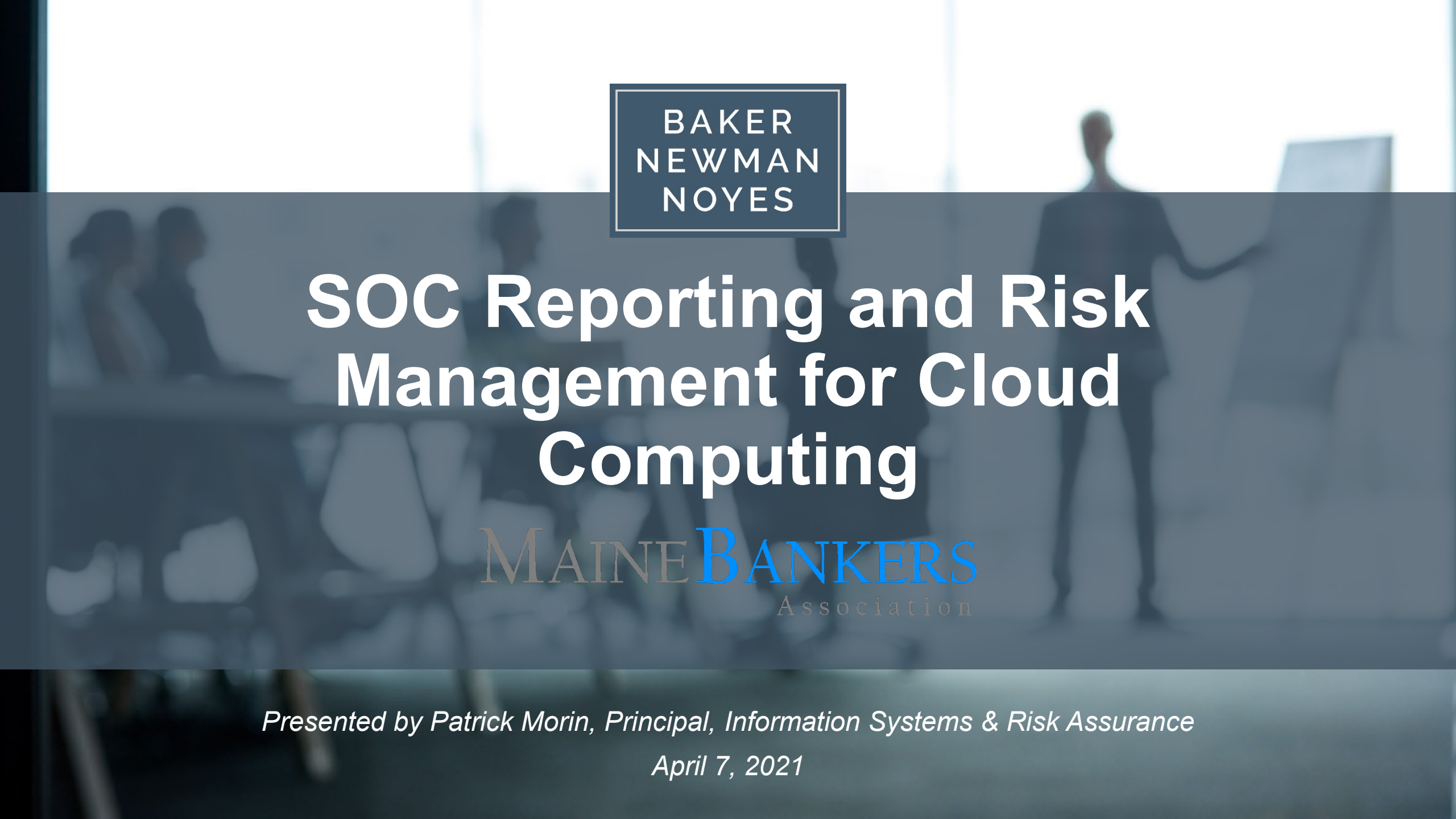


BAKER NEWMAN NOYES

SOC Reporting and Risk Management for Cloud Computing

MAINE BANKERS Association

Presented by Patrick Morin, Principal, Information Systems & Risk Assurance

April 7, 2021

Here with you today.

PATRICK MORIN, CPA, CISA, CISM, CITP

- Information Systems and Risk Assurance Principal
- pmorin@bnncpa.com
- 207.791.7188

Learning Objectives

SOC Reports

- Distinguish between SOC 1®and SOC 2®reports
- Identify elements for review within applicable SOC reports
- Determine if additional due diligence is needed over service organizations

Cloud Computing

- Evaluating risk management for cloud computing over five key areas

Comparing SOC for Service Organizations Reports

BAKER NEWMAN NOYES

SOC 1	SOC 2
Focus of Report	
Internal control over financial reporting Evaluate the risks related to financial reporting	Evaluate the risks related to the achievement of specified service commitments and system requirements (i.e. SLAs) Security, availability, processing integrity, confidentiality, or privacy (Trust Services Criteria)
Scope and Subject Matter of Report	
The system, relevant services and control objectives	The system and the related controls that achieve the service commitments and system requirements.

Comparing SOC for Service Organizations Reports (cont.)

SOC 1	SOC 2
Purpose of Report	
Audit of financial statements	Oversight, due diligence
Intended Users	
Management of the service organization, user entities, and auditors of the user entities' financial statements	Management of the service organization and user entities and business partners, ***prospective user entities and business partners***, and regulators who have sufficient knowledge and understanding.

Comparing SOC for Service Organizations Reports (cont.)

BAKER NEWMAN NOYES

SOC 1	SOC 2
Who might need the report?	
• Payroll service providers • Trust administrators • Benefit plan administrators • Health care claims management processors* • Financial reporting system hosting provider*	• Enterprise IT outsourcing • Sales force automation • Managed security providers • Customer support providers • Cloud-based solution providers (SAAS; PAAS)

* Some organizations might obtain and share both SOC 1 and SOC 2 reports

Comparing SOC for Service Organizations Reports (cont.)

BAKER NEWMAN NOYES

SOC 1	SOC 2
Report components	
A description of the service organization's system • Control objectives • ICFR	A description of the service organization's system • Service commitments and system requirements • Trust services criteria
Management's assertion	

Comparing SOC for Service Organizations Reports (cont.)

BAKER NEWMAN NOYES

- There are two types of SOC 1 and SOC 2 reports:

A report on …	Type 1	Type 2
Management's description of the service organization's system	As of a specified date	Throughout a specified period
The suitability of the design of the controls		
The operating effectiveness of the controls	N/A	

Comparing SOC for Service Organizations Reports (cont.)

BAKER NEWMAN NOYES

- There are two types of SOC 1 and SOC 2 reports (cont.):

Descriptions of	Type 1	Type 2
Controls in place to achieve: • The control objectives (SOC 1) • Service commitments and system requirements (SOC 2)	As of a specified date	Throughout a specified period
A description of the service auditor's tests of the controls and the results of the tests	N/A	

What to Review in a SOC Report

- The service auditors' report
- The content of the description
- The control objectives specified by management (SOC 1)
- The trust services categories selected by management (SOC 2)
- Any testing exceptions noted in the report
- Any complementary user entity controls (CUECs) or complementary subservice organization controls (CSOCs) specified in the report

Review the Service Auditors' Report

- Review the type of opinion
  - Unqualified
  - Qualified (look for a statement that includes "except for")

- If anything other than unqualified, review the impact of the qualifications and the exceptions noted

Inspect the System Description

- Contains the following:
  - Relevant aspects of the control environment

SOC 1	SOC 2
A description of the services provided	A description of the system The principal service commitments and system requirements
The control objectives and relevant controls	Applicable trust services criteria and relevant controls

Confirm the report is the for the correct service provider location.

  - In a type 2 report, the control objectives and relevant controls (SOC 1) or the applicable trust services criteria and relevant controls (SOC 2) may be alternatively presented in the description of the service auditor's test of controls.

SOC 1: Content of the Description

- The system description should include the following:
  - The related accounting records and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions
  - How the system captures and addresses significant events and conditions other than transactions
  - The process used to prepare reports and other information for user entities
  - Relevant IT general controls that support the system
  - A description of the relevant aspects of the control environment
  - A description of any changes during the reporting period
  - When applicable:
    - Complementary user entity controls (CUECs)
    - Complementary subservice organization controls.

SOC 2: Content of the Description

- The system description should include the following:
  - The types of services provided
  - The principal service commitments and system requirements (i.e. SLAs)
  - The components of the system used to provide the services
    - Infrastructure
    - Software
    - People
    - Procedures
    - Data
  - The boundaries or aspects of the system covered by the description

SOC 2: Content of the Description (cont.)

BAKER NEWMAN NOYES

- The system description should include the following:
  - A description of the relevant aspects of the control environment
  - Third-party access to the system and its data
  - The nature, timing, and extent of identified any incidents that
    - were the result of controls that were not suitably designed or operating effectively
    - otherwise resulted in a significant failure in the achievement of any service commitments and system requirements, as of the date of the description (type1) or during the period covered by the description (type 2)
  - Any applicable trust services criteria that are not addressed by a control and the reasons

SOC 2: Content of the Description (cont.)

BAKER NEWMAN NOYES

- The system description should include the following:
  - Relevant details of changes to the service organization's system during the period (type 2)
  - The applicable trust services criteria and the related controls designed to meet those criteria, including aspects of the overall control environment
  - When applicable
    - Complementary user entity controls (CUECs)
    - Complementary subservice organization controls (CSOCs)

Evaluate the Results of Testing

- Did the service organization provide a **Type 2** report?

- The results of the service auditors' testing are presented after the description of the system in the report. Consider reviewing:
  - Any testing exceptions for applicability/impact to your organization
  - Review any included management's response(s) for remediation efforts
  - The sufficiency of test procedures for your concerns

Evaluate CUECs and CSOCs

- CUECs
  - Controls the service organization assumes are implemented by user entities (you)
    - Review for relevance to your organization
    - Confirm that your organization has implemented relevant control(s)

- CSOCs
  - Controls the service organization assumes, in the design of their system, will be implemented by the subservice organizations and are necessary to achieve the control objectives (SOC 1) or service commitments/system requirements (SOC 2)
    - Review for relevance to your organization
    - Consider obtaining the subservice organization's report

Evaluate the Presentations of Subservice Organizations

BAKER NEWMAN NOYES

When applicable, the description should include information about subservice organizations:

Relationship	Presentation	Oversight
• Is it a third party or related to the service organization?	• Is the service organization using the carve-out method or the inclusive method?	• How is the organization monitoring that controls are present and operating at subservice organization?

As a downstream user organization of your service organization's subservice organization, a determination should be made if the controls performed by the subservice organization are considered significant. If so, you should consider requesting a copy of the subservice organization's SOC report(s).

Recently Added SOC Reports

- SOC for Cybersecurity
  - A reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs.

- SOC for Supply Chain
  - A reporting framework for controls over a manufacturing, production, or distribution system.
    - Supply chain risk+- management efforts
    - Processes and controls to detect, prevent, and respond to supply chain risks
    - Management-prepared system information

BAKER NEWMAN NOYES

SOC Reporting - Questions

BAKER NEWMAN NOYES

Cloud Computing

MAINE BANKERS Association

Presented by Patrick Morin, Principal, Information Systems & Risk Assurance

April 7, 2021

Learning Objectives

SOC Reports

- Distinguish between SOC 1®and SOC 2®reports
- Identify elements for review within applicable SOC reports
- Determine if additional due diligence is needed over service organizations

Risk Management over Cloud Computing

- Evaluating risk management for cloud computing over five key areas

Cloud Computing:
Importance of Due Diligence

- False Assumption:

  Assuming effective security and resilience controls exist because the technology systems are operating in a cloud computing environment

- You've Heard it Before:

  Regardless of the system used, ***the financial institution is ultimately responsible*** *for the safety and soundness of cloud services and the protection of sensitive customer information.*

Cloud Computing Risk Considerations

- **The function outsourced**
  - Sensitivity of data accessed, protected, or controlled by the service provider
  - Volume of transactions
  - Criticality to the financial institution's business
  - The agreement on the division of responsibilities

- **The technology used**
  - Reliability
  - Security
  - Scalability to accommodate growth

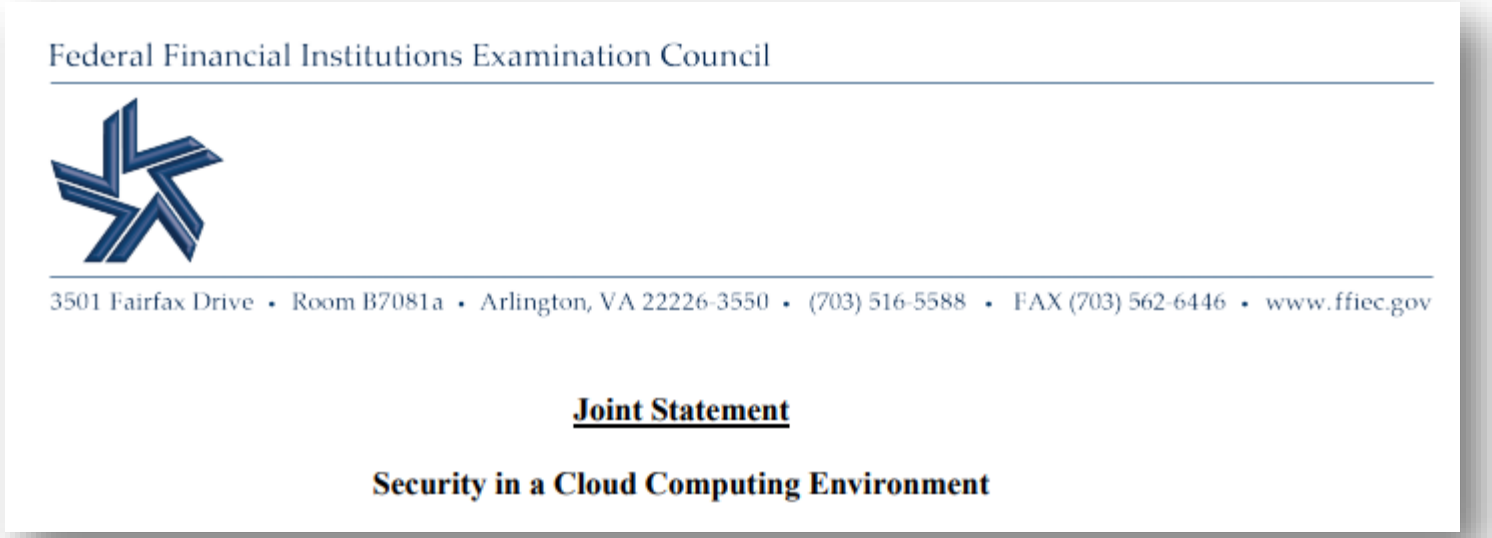
Cloud Computing Risk Considerations (cont.)

BAKER NEWMAN NOYES

- **The service provider**
  - Strength of financial condition
  - Turnover of management and employees
  - Ability to maintain business continuity
  - Ability to provide accurate, relevant, and timely Management Information Systems
  - Experience with the function outsourced
  - Reliance on subcontractors
  - Location, particularly if cross-border
  - Redundancy and reliability of communication lines

Cloud Computing:
Five Key Areas of Risk Management

- Governance
- Cloud Security Management
- Change Management
- Resilience and Recovery
- Audit and Controls Assessment



Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • www.ffiec.gov

Joint Statement

Security in a Cloud Computing Environment

BAKER NEWMAN NOYES

Cloud Computing – Governance

Align	Align the FI's overall strategy, IT strategy, IT architecture and risk tolerability with the use of cloud computing services.
Considerations	Determine the appropriate level of governance, the types of systems and informational assets that will be utilized for these services.
Impact	Determine the impact to the FI architecture, operations model and ability to monitor these services.

Cloud Computing – Cloud Security Management

BAKER NEWMAN NOYES

- Security Management and Oversight
- Contractual Responsibilities
- Inventory Identification and Management
- User Access Provisioning and Permission Levels
- Data Loss Prevention
- End User Training

Cloud Security Management:
Security Management and Oversight

Identify Risks	Identify security related risks during the planning, implementation, and selection of a cloud service provider
Implement Controls	Implement appropriate control processes to mitigate identified risks once an agreement is in place
Test	Identify control effectiveness by testing or auditing the cloud service provider's security controls. This can be done by leveraging a SOC report.
Monitor	Implement and monitor the security tools and configuration management capabilities provided by the cloud service provider to ensure that all risks are mitigated.

Cloud Security Management:
Contractual Responsibilities

BAKER NEWMAN NOYES

- Ensure the Contractual Agreement includes:
  - Service level expectations
  - Control responsibilities of the provider
  - Control responsibilities of the Financial Institution (FI)

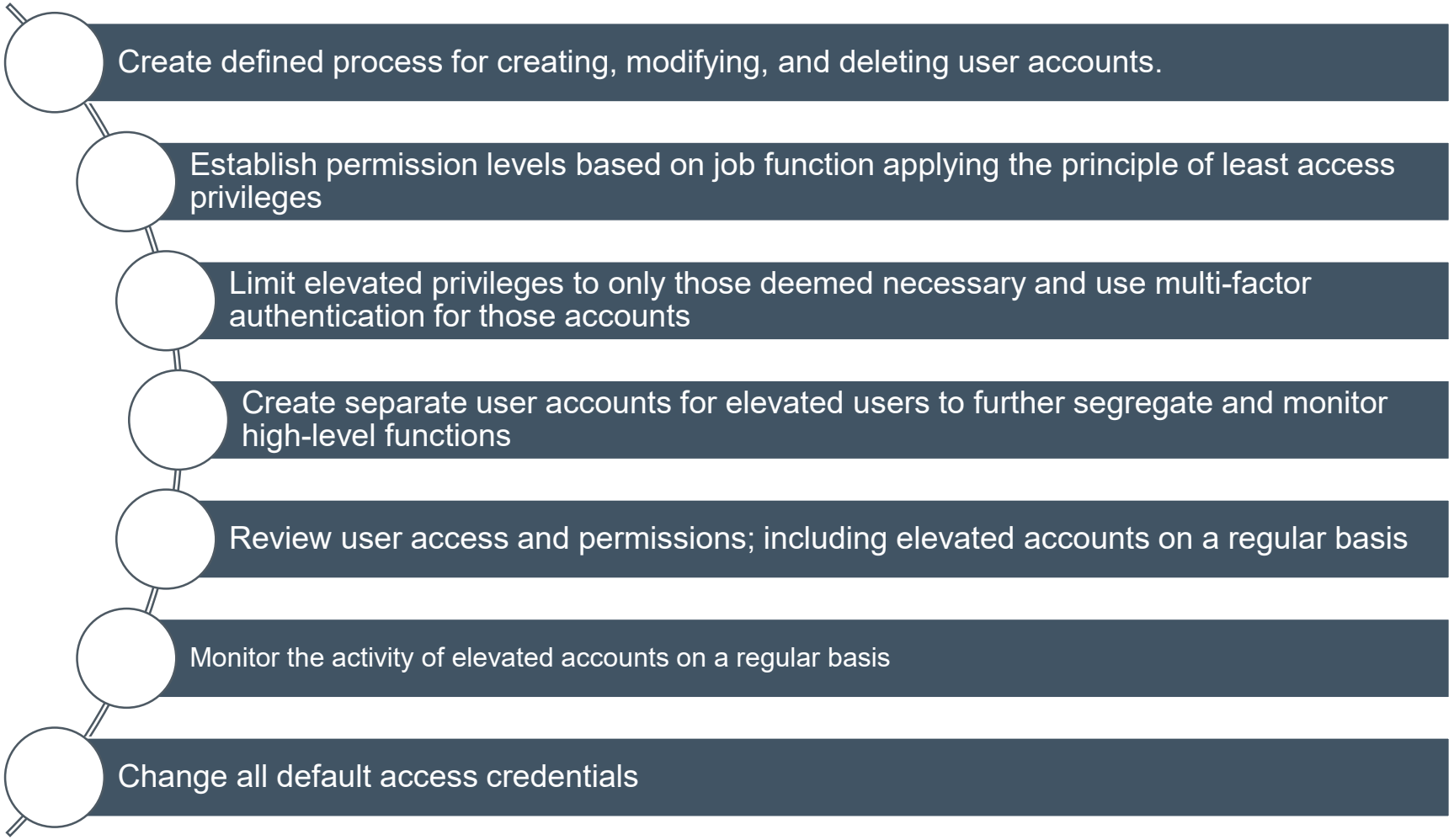
- Consider the need for additional controls to maintain security standards of the FI

Cloud Security Management:
Inventory Identification and Management

- Determine the information and system types that will be migrated to your cloud computing environment

- Create inventory management procedures to account for all systems and information; including virtual machines, firewalls, and network devices to ensure better management and safeguarding of information

Cloud Security Management:
User Access Provisioning and Permission Levels



Cloud Security Management:
Data Loss Prevention

- Implement encryption and data tokenization where applicable
- Create a defined process for encryption key management between the cloud service providers and FI. Encryption key management systems are often offered by the cloud provider but beware that they may allow an administrator from the cloud provider access to the information
- Establish clear communication between both parties to identify the best controls for protection of sensitive data

Cloud Security Management:
End User Training

BAKER NEWMAN NOYES

- According to Oracle University, "**End user adoption is the primary determinant of whether a cloud implementation is successful.**"
- FIs should seek out trainings specific to the cloud environment and require attendance by all users
- Trainings should be done by all users at every major release or update
- Trainings can be obtained by:
  - External organizations on cloud technology
  - Product specific trainings provided by the cloud service provider

Cloud Computing – Change Management

BAKER NEWMAN NOYES

- Update current Change Management to reflect current procedures regarding the cloud computing environment and confirm the procedures are documented and detailed.
- Ensure Change Management controls are in the contractual agreement with the cloud service provider and responsibilities are clearly stated. Additionally, change management controls can be found within a SOC report.
- If the FI employs a micro-service architecture, ensure that established change management procedures are implemented throughout the entire environment to include all micro-services.

Cloud Computing – Resilience and Recovery

BAKER NEWMAN NOYES

- Business Continuity (BC) and Disaster Recovery (DR)
- Incident Response Capabilities

Cloud Computing – Resilience and Recovery (cont.)

BAKER NEWMAN NOYES

- Business Continuity and Disaster Recovery
  - Understand the resilience capabilities and service options available from the cloud service provider.
  - Review the contract to ensure resilience and recovery options are included in the cloud service offerings, or research the available add-on options from the provider.
  - Evaluate and determine how the cloud affects both the BC and DR
  - Update the current BC and DR to reflect current cloud services and changes to configurations
  - Regularly test and validate resilience and recovery capabilities

Cloud Computing – Resilience and Recovery (cont.)

BAKER NEWMAN NOYES

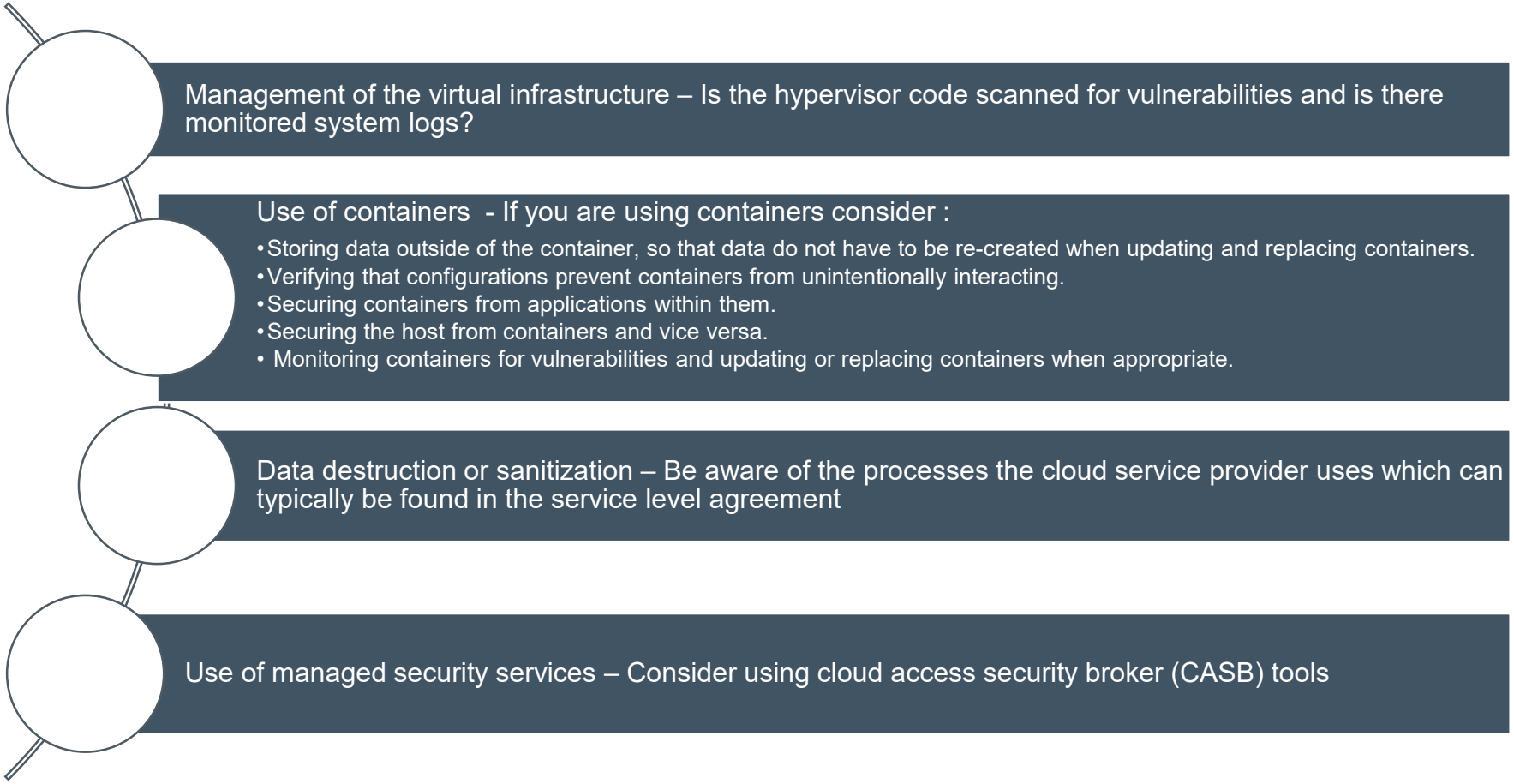
- Include cloud-specific challenges due to ownership and governance of technology assets owned or managed by the cloud service provider within Incident Response
- Ensure contract defines responsibilities regarding incident reporting, communication, and forensics to both the provider and the FI
- Thoroughly review the service level agreement for identification of providers responsibilities for incident response and in an event of an incident
- Many cloud service providers offer monitoring and alerting tools that can be used by the FI, and integrated into its incident response plan

Cloud Computing - Audit and Controls Assessment

BAKER NEWMAN NOYES

Internal Monitoring	• Establish practices with external assessors or the internal audit function to perform regular audit and testing of security controls that have been implemented to secure the cloud computing environment.
External Monitoring	• Evaluate and monitor the cloud service provider's technical, administrative and physical security control environment that is used to support the FI's cloud computing services. This can include reviewing internal assessments and security reports and implemented policies and procedures such as internal audit reports, penetration testing, and vulnerability scans, written information security plans, and business continuity and disaster recovery plans. • Establish practices for obtaining and reviewing external audit reports over the cloud computing services, including SOC reports and ISO certification reports, to gain assurance that controls within the cloud service provider are implemented and operating effectively.

Controls Unique to Cloud Computing



General Discussion and Questions