

# Considerations When Moving ERP to the Cloud

Steve Shofner, Senior Manager,  
Armanino LLP

Governance, Risk & Compliance – G24



The background of the slide features a stylized cityscape with silhouettes of buildings and bridges, including the Golden Gate Bridge, against a warm, yellowish-orange sky. The word "CyberSizelT" is prominently displayed in the foreground in a large, red, outlined font. The "C" and "T" are significantly larger than the other letters.

# Learning Objectives

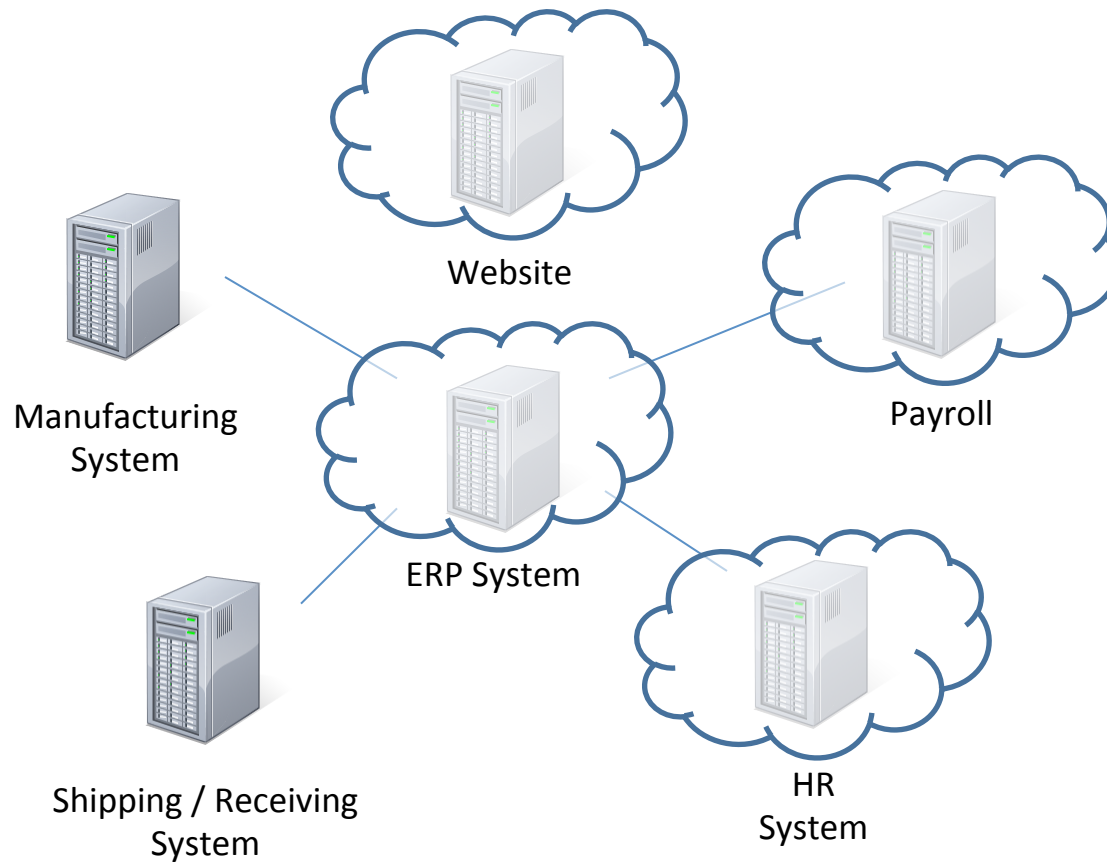
- Review key system selection considerations
- Analyze important security concerns of having your data in the cloud
- Evaluating Cloud Hosting Providers
  - Up Front
  - Ongoing



# Why Organizations Outsource

- Most organizations seek vendor services because the vendor:
  - Has needed expertise
  - Has capacity
  - Assumes risk (has good controls)
  - Perform at scale (at a lower cost to each customer)

# Solutions For Cloud Apps

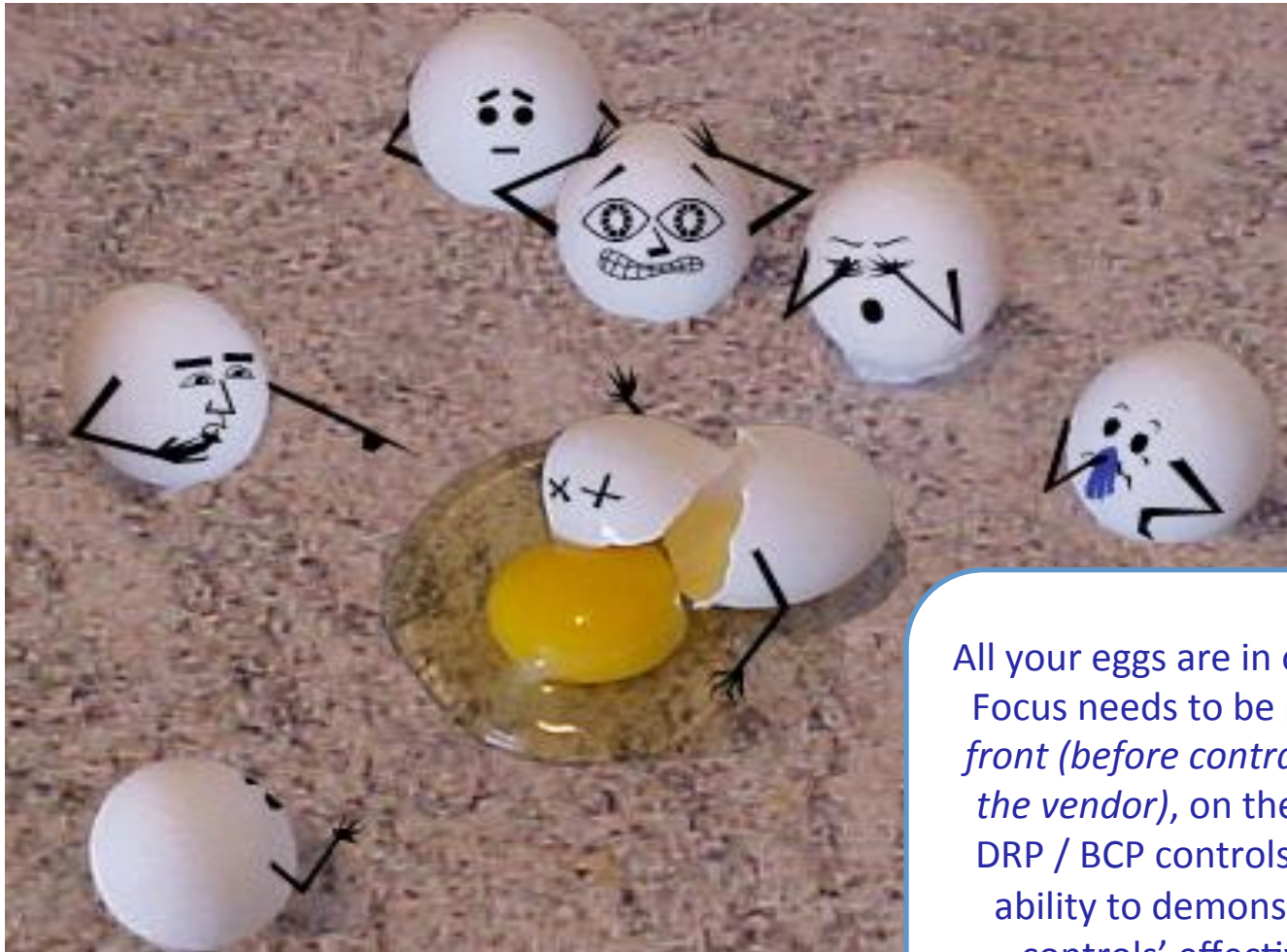


# Outsourcing Tasks vs. Responsibility

- Balancing Control vs. Cost
- When outsourcing, you are still responsible for ensuring controls are in place
  - You're delegating the *task*, not the *responsibility*
  - If the hosting company allows corruption of your company's data, it's your company that will bear the reputation damage and other problems/costs!
- **Good News!** Most hosting companies are actually controlled *better* than individual companies!



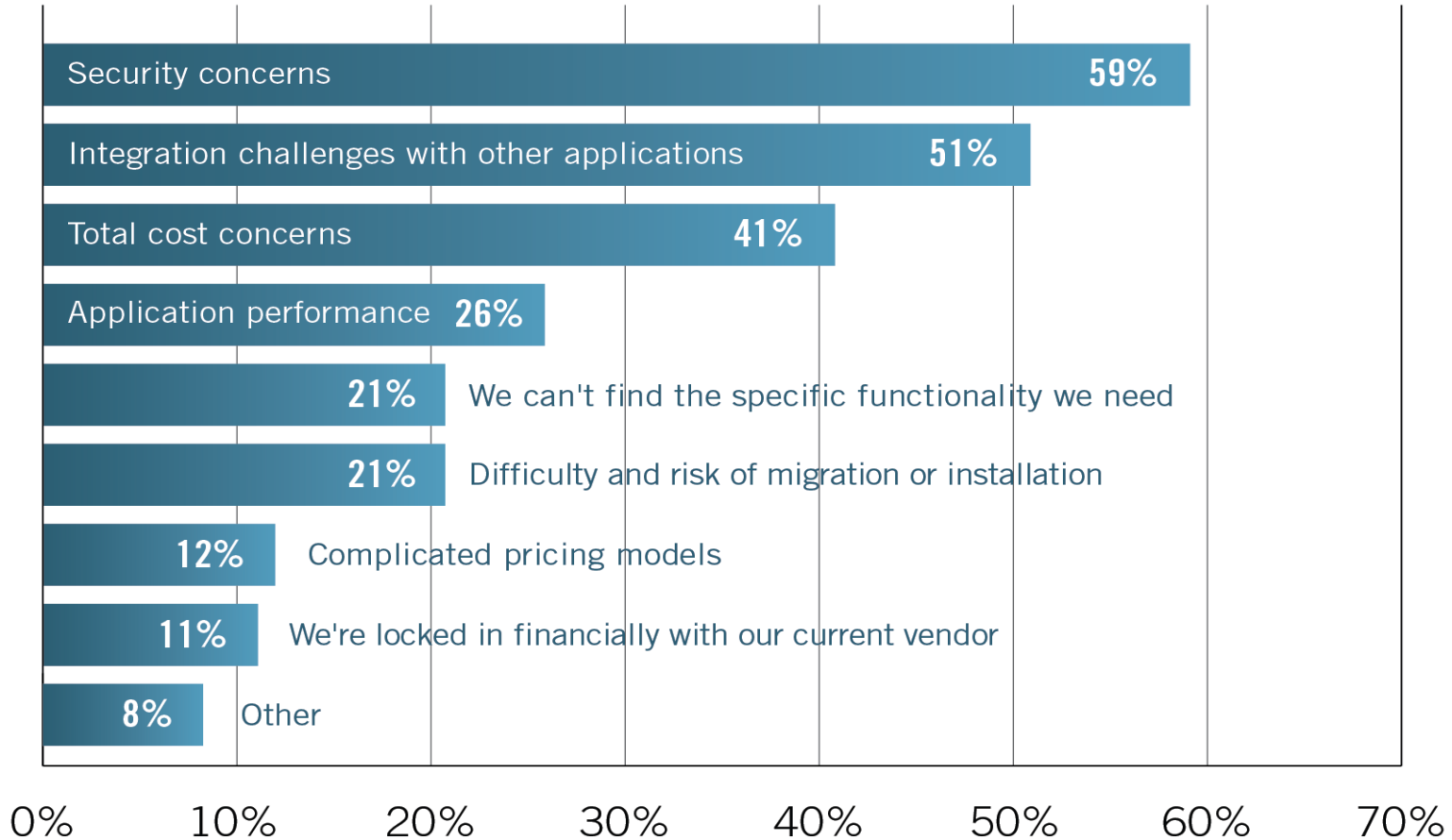
# Reliance On Others



All your eggs are in one basket. Focus needs to be placed, *up front (before contracting with the vendor)*, on the vendor's DRP / BCP controls and their ability to demonstrate the controls' effectiveness.

# Top Challenges

What are your top concerns about cloud computing?



# Concern Call-Out: Security



**CLOUD ACCOUNTING**  
INSTITUTE

- Moved up to #1
- Potential reason ~ recent press about big-name security breaches have this top of mind

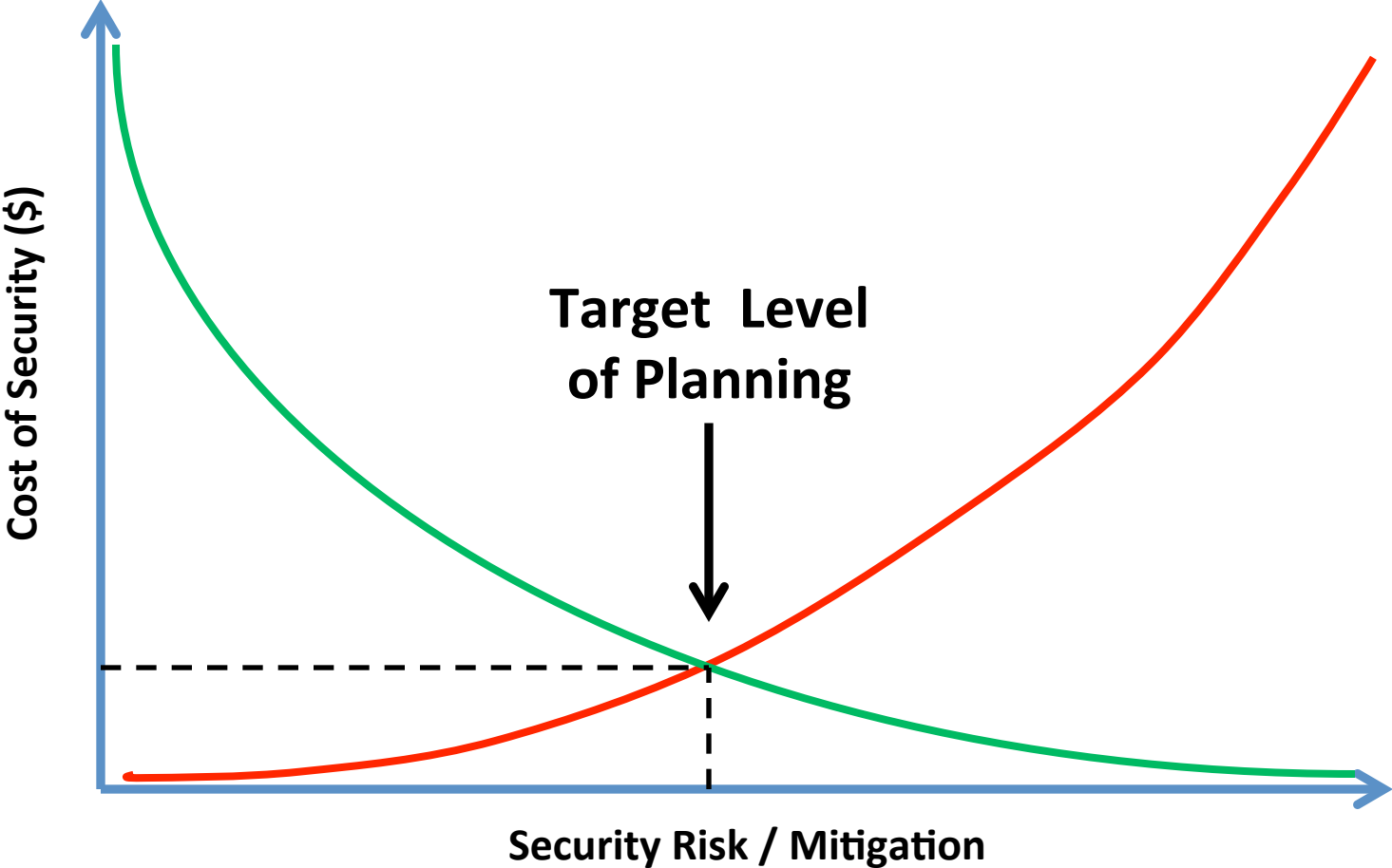


# An Example: Cumulative Security Benefit



- Security is a form of insurance. More is better, but there is a cost
- How much is enough?

# How Much Security Is Enough?



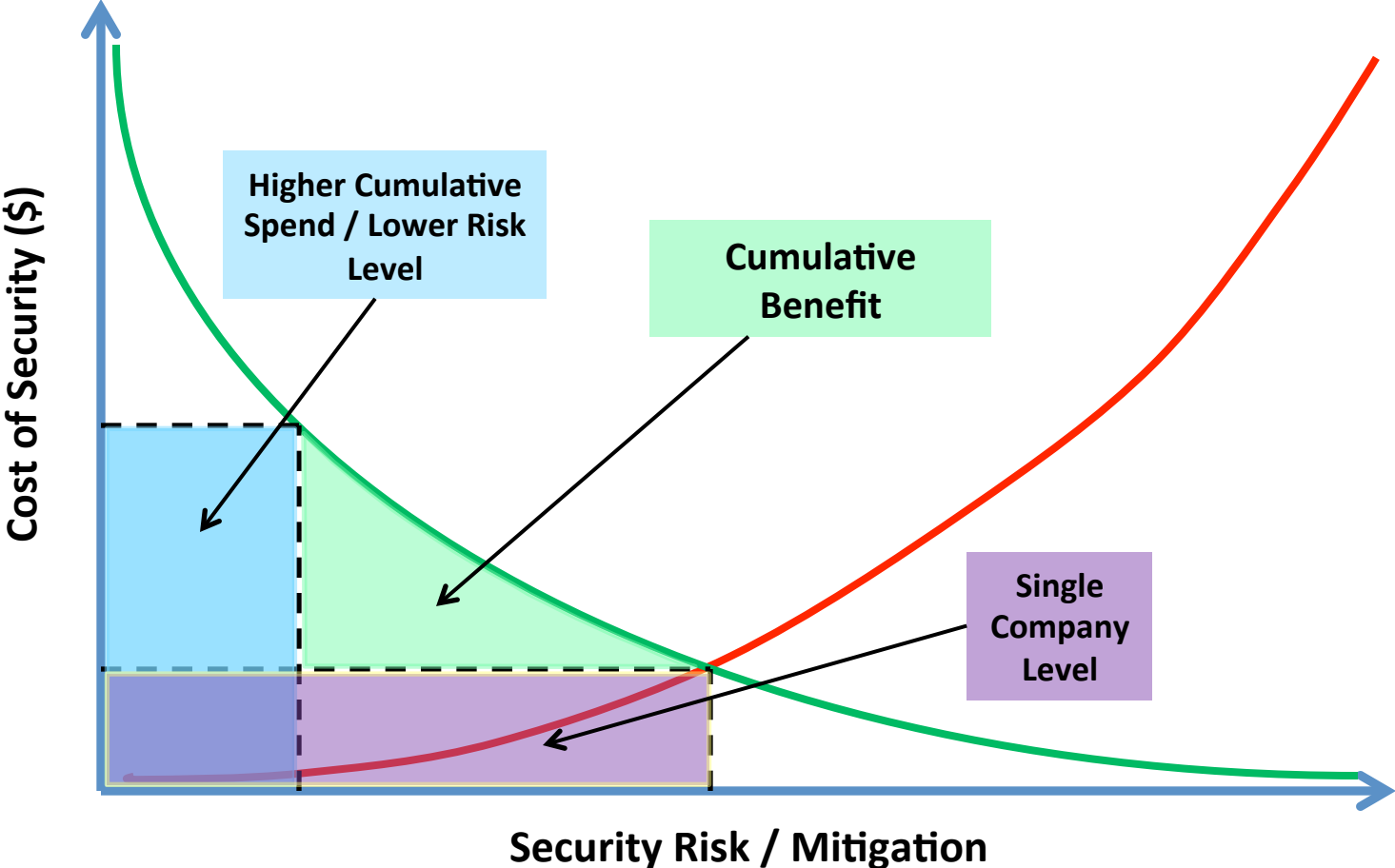
# How Much Security Is Enough?

Hosted environments tend to be more secure than individual companies. They invest more in security, resulting in a more secure environment



# How Much Security Is Enough?

## Cumulative Benefit



# Hosting Benefits: More Than Just (Physical) Security

- System / Network Security
  - User Administration (adding, modify, removing, monitoring users)
  - System Hardening
  - Network / System Monitoring
  - Robust Security Response
- IT Operations
  - Job Scheduling
  - Monitoring
  - Problem / Incident Response
  - Backups
  - Offsite Storage Rotation
  - Disaster Recovery / Business Continuity Plans
- System Development Lifecycle (SDLC) / Change Management
- Patch Management (Operating Systems, Databases, Network, etc.)
- Help Desk / Service
- Environmental Safeguards
  - Fire Suppression
  - Leak Detection
  - Redundant Power Sources
  - Uninterruptable Power Supplies (UPS)
  - Power Conditioners
  - Generators
  - Redundant Network Providers

# Ensuring Controls

- Remember - Task vs. Responsibility
  - *You need to ensure good controls are operating effectively*
- Perform Due Diligence Up-Front
  - Contract
  - Service Level Agreement (SLA)
  - Audit Clause (Giving You The Right To Audit)
  - Code escrow
  - Ability to perform own backups
  - Availability of a Type II Service Organization Control (SOC) Report
  - Etc.
- Regular Assessments (At Least Annually)
  - Monitor Performance Metrics / Reports
  - Perform Independent Audits
  - Re-Review Contracts (and Issue Change Orders, If Needed)

# DUE DILIGENCE – UP FRONT



*Trust in, and value from, information systems*

**San Francisco Chapter**

A stylized silhouette of the San Francisco skyline is shown against a light, hazy background. The Golden Gate Bridge is the most prominent feature on the left, with its towers and suspension cables. Other buildings and bridges are visible in the background.

# CyberSizeIT



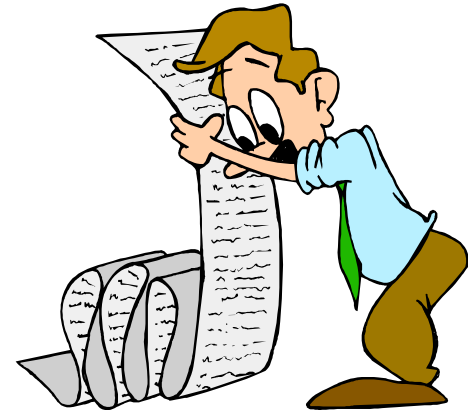
# Due Diligence

- Contract Terms:
  - Description of the service provided
  - Duration
  - Renewal (e.g., Auto, Annually, other)
  - Responsibilities of each party
  - Change Order Process
  - Service Level Agreements / Metrics
  - Guarantees
  - Fees
  - Assumptions
  - Payment Terms
  - Termination
  - Conflict Resolution
  - Provisions Allowing Audits
  - Availability of SOC Reports
  - Intellectual Property
  - Non-Disclosure
  - Confidentiality
  - Required Breach Notification
  - Data Retention & Destruction
  - Conflict Resolution (e.g., Mediation / Arbitration)
  - Limitation of Liability
  - Code Escrow



# Due Diligence

- Perform Checks
  - Background
  - Reference
  - Financial
  - Company Viability
  - Reputation
  - Criminal (if appropriate)
  
- Assess Risk
  - Obtain and evaluate latest audit report(s)
  - Create and have vendors complete a questionnaire



# Regular Assessments

- Monitor Performance
  - Metrics
  - Reporting
- Perform Independent Audits
  - Directly
  - Service Organization Controls (SOC) Reports
  - Other Independent Sources: e.g., Agreed-Upon Procedures (AUP), Payment Card Industry (PCI) Assessments, Health Information Portability and Accountability (HIPAA) Assessments, etc.

# Regular Assessments

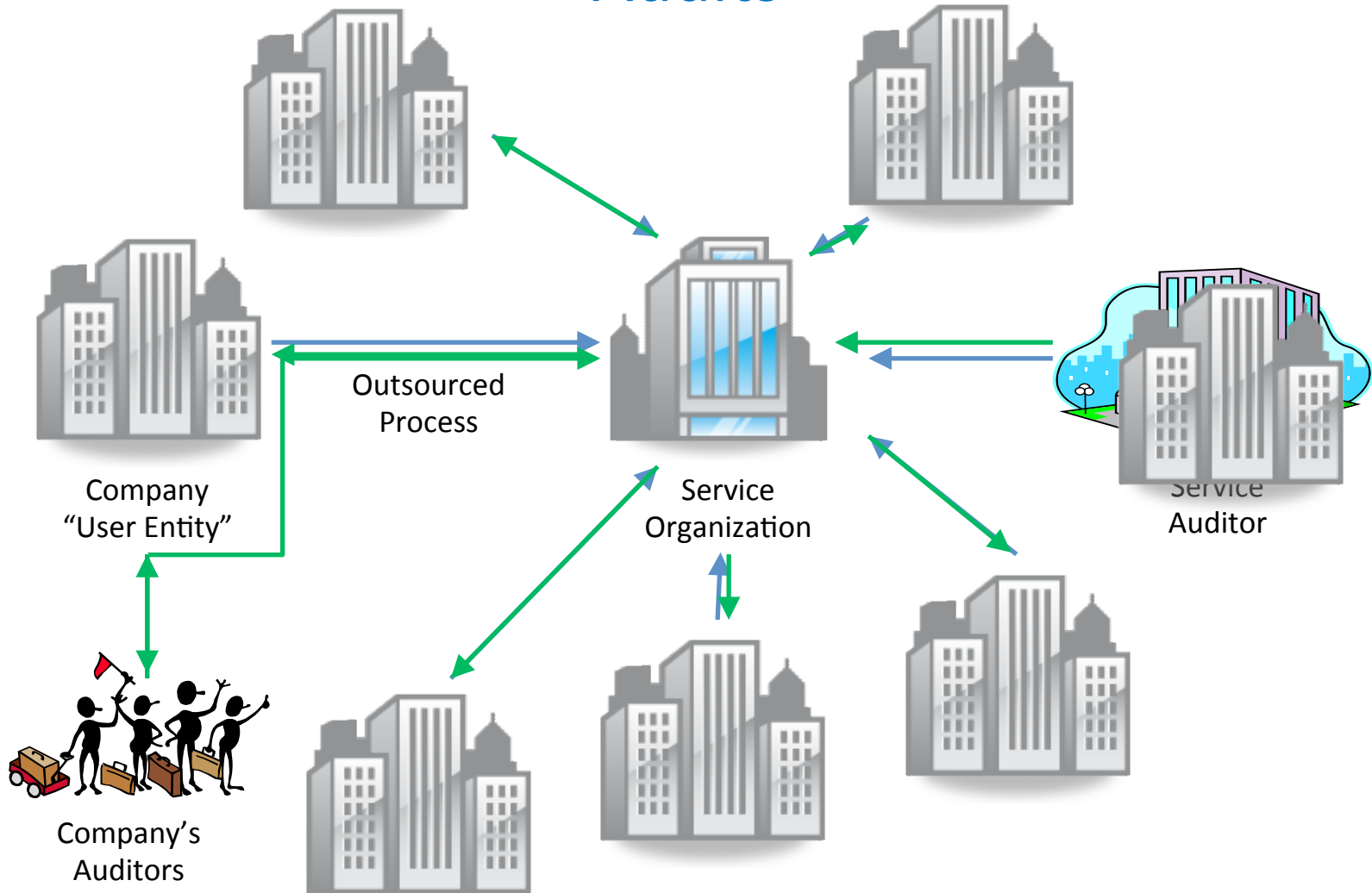
- Contract Review / Renewal
  - Depends on the terms agreed-upon
  - May need to negotiate Change Orders?

# REGULAR ASSESSMENTS - SERVICE ORGANIZATION CONTROLS (SOC) REPORTS?



The "CyberSizeIT" logo is rendered in a large, stylized font with a red-to-orange gradient and a white outline. The background of the slide features a silhouette of a city skyline with a prominent suspension bridge, likely the Golden Gate Bridge, set against a warm, yellowish-orange sky.


# Outsourcing and The Need For Independent Audits



# Dispelling Myths

- The Existence of a SOC report does **not** mean the vendor is “SOC Certified”
- SSAE 16 and AT 101 are **Audit** Standards regarding how auditors do their work
  - How to audit
  - How to report results
- SOC reports are **audit reports** (not “certifications”), which could include bad results (poor controls, test exceptions, control failures, etc.) ...and many reports do
- It is incumbent upon User Entities to read the reports, make sure they address their needs, determine if they identify any issues or problems, and address any gaps or risks identified

# Service Organization Controls (SOC) Reports

	SOC 1	SOC 2	SOC 3 
<b>Purpose</b>	Report on Financial Statement Processes & Controls	Report on Compliance or Operations	Report on Compliance or Operations
<b>Addresses</b>	Financial Statement Processes & Controls	<b>Trust Services Principles &amp; Criteria</b>	
		Security, Confidentiality, Processing Integrity, Availability, and/or Privacy Controls	Security, Confidentiality, Processing Integrity, Availability, and/or Privacy Controls
<b>Professional Standard</b>	SSAE 16	AT 101	AT 101
<b>Use</b>	Restricted Use Report	Usually a Restricted Use Report	General Use Report, with a Public Seal

# Structure of SOC 1 and SOC 2 Reports

- There are five sections:
    1. Service Auditor's Opinion Letter
    2. Management's Assertion Letter
    3. Description of Controls
    4. Testing Results
    5. Other Information
- ← Not Audited
- Critical information is spread throughout the report



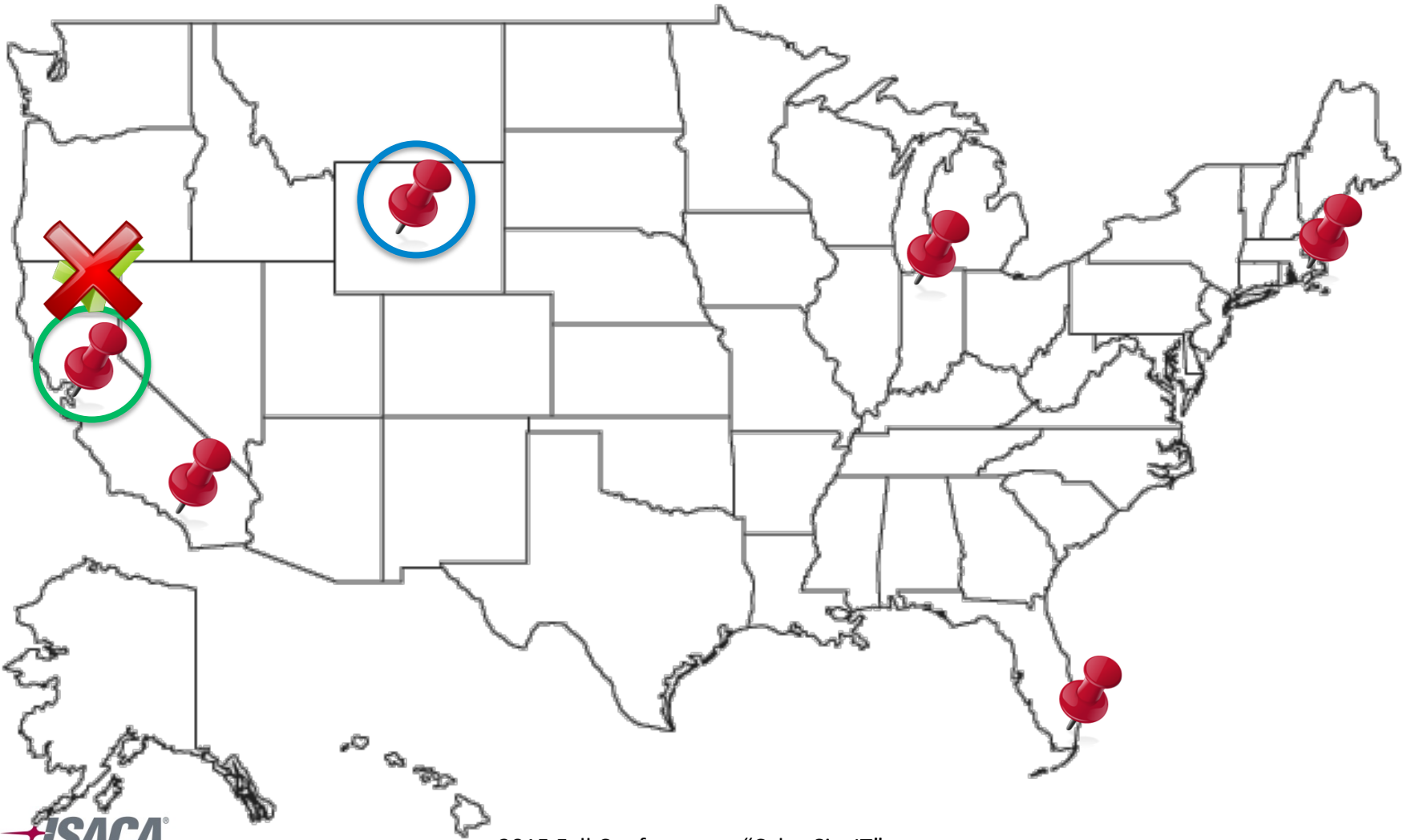
# Evaluating SOC 1/2 Reports

- Are there Client Control Considerations?
  - These are controls that the Service Organization tells *you* to have for the overall control environment to be effective
  - They are usually at the end of Section 3, but could be peppered throughout the report
  - You need to establish these controls *in your organization* and monitor (test) them to ensure their ongoing operational effectiveness

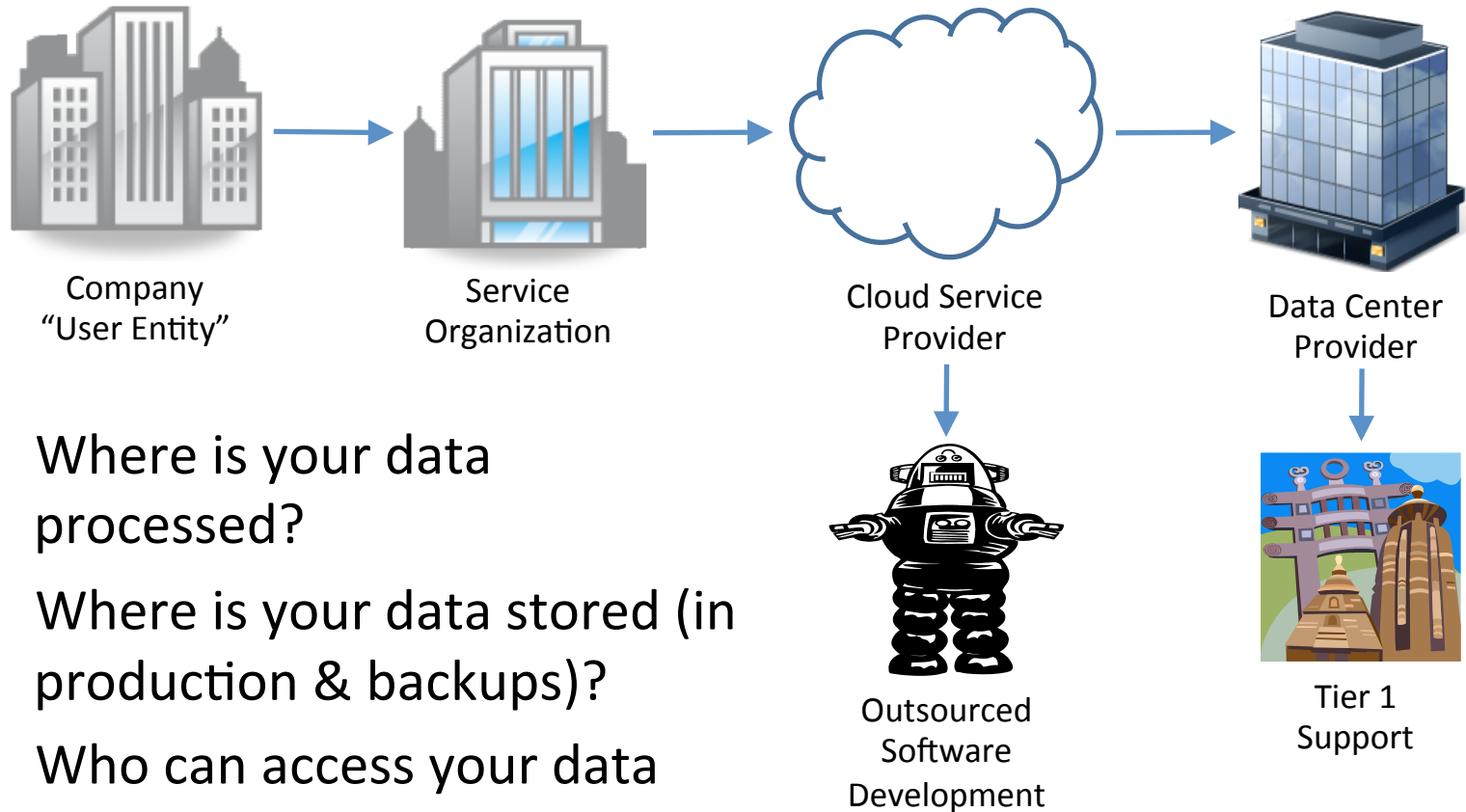
# Evaluating SOC 1/2 Reports

- Determining Coverage:
  - Does the report cover the service you are purchasing?
    - The Specific Application(s)
    - Processing Centers / Data Centers
    - Cities / Countries

# Geographic Coverage



# Sub-Service Providers



1. Where is your data processed?
2. Where is your data stored (in production & backups)?
3. Who can access your data (and from where)?

# Evaluating SOC 1/2 Reports

- Are there any Sub-Service Providers?
  - The report will either be “Inclusive” or “Carve Out” those sub-services provider’s processes and controls
- If it is the Carve Out approach, the Sub-Service Provider’s SOC Report must also be addressed:
  - Obtain and evaluate *their* SOC report, and/or
  - Perform an audit of the Sub-Service Provider, as if they were an extension of the User Organization

# Evaluating SOC 1/2 Reports

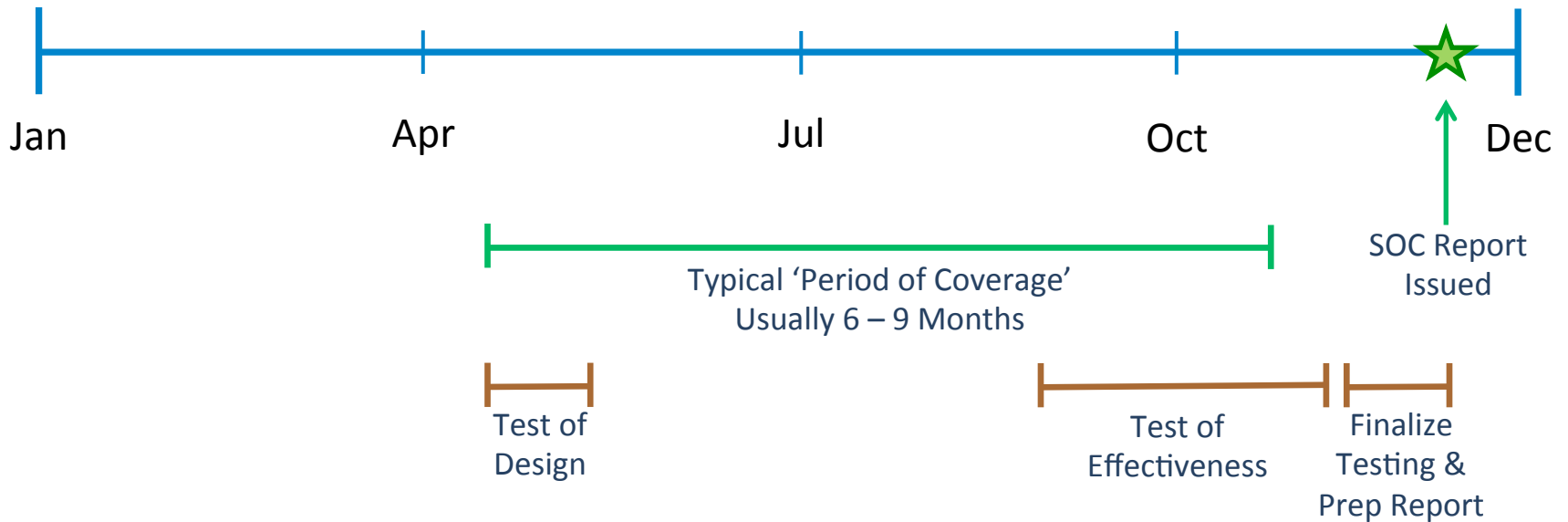
- Is the report the right Type?

	Type I	Type II
<b>Period of Coverage</b>	Point In Time Only	Period of time. Typically a minimum of six months
<b>Testing Performed</b>	No	Yes
<b>Value of the Report</b>	Provides a description of controls that have been evaluated by the Service Organization, and an opinion regarding the <u>design of controls</u> only.	Has all the information noted in a Type I, and it includes testing of the controls for the period of time specified. The opinion is regarding the <u>design of controls</u> <i>and</i> the <u>operational effectiveness of controls</u> for that period of time.

# Evaluating SOC 1/2 Reports

- Does the Period of Time meet your needs?
  - Point in time (Type I)
  - Period of time (Type II)
- SOC Reports are typically used to support User Entity audits (including their external audits). If so, does the report provide sufficient coverage to meet the audit's needs?

# Typical Type 2 Timeline



- Does this provide enough coverage for your organization (consider your fiscal year)?
- You may need to request a “Bridge Letter” from the vendor



# Evaluating SOC 1/2 Reports

- Is there a “Qualified” opinion?
  - Basically says “These processes and controls are good... well, let me qualify that. They are good, *except for...*”
  - You want an “Unqualified” opinion
- Was there an Adverse Opinion?

# Evaluating SOC 1/2 Reports

- Are Any Controls Missing?
  - Depending on *your* organization's control strategy, you may *require* certain controls, but the Service Organization may not have them
  - Remember SOC reports are not “certifications.” There are no ‘required’ controls.

# Evaluating SOC 1/2 Reports

- Were there any Exceptions noted during testing?
  - You need to establish these controls *in your organization* and monitor (test) them to ensure their ongoing operational effectiveness

# Evaluating SOC 1/2 Reports

- For any Missing Controls, Client Control Considerations, or Testing Exceptions, you need to determine how to address the related risks:
  - Implement controls at the User Entity (your organization)
  - Convince the Service Organization to implement new controls
  - Switch to another Service Organization

# SOC Review Summary:

- Determine Scope & Coverage
  - The Specific Application(s)
  - Processing Centers / Data Centers
  - Cities / Countries
  - Type I or II
  - Date Coverage
  - Use of Sub-Service Providers (inclusive or carve-out)
- Check for Control Issues:
  - Adverse and/or Qualified Opinion
  - Missing Controls
  - Client Control Considerations
  - Testing Exceptions
- Evaluate & address impact to your organization

# RESOURCES



*Trust in, and value from, information systems*

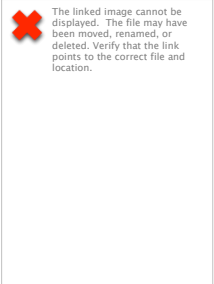
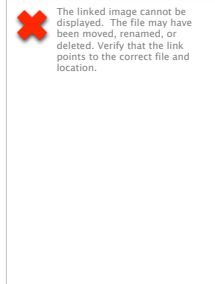
**San Francisco Chapter**

A stylized illustration of the San Francisco skyline, including the Golden Gate Bridge, the Transamerica Pyramid, and other buildings, set against a warm, yellowish-orange background.

# CyberSizeIT

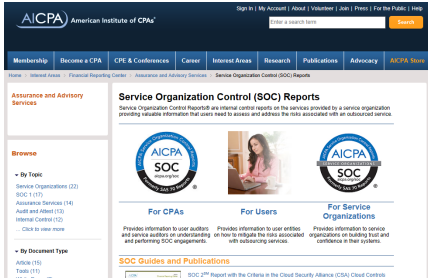
# Resources

- AICPA:
  - Books:



- Website:

- SOC Report Info & Guidance:
- <http://www.aicpa.org/soc>



- ISACA Book: Vendor Management



- Armanino Whitepaper: Evaluating SOC Reports
  - Sent email to [Steve.Shofner@amllp.com](mailto:Steve.Shofner@amllp.com) to request a copy.



**Questions?**





**Steve Shofner, Senior Manager**  
**Governance, Risk, & Compliance IT Team Leader**

email: [Steve.Shofner@amllp.com](mailto:Steve.Shofner@amllp.com)

Office: (925) 790-2879

Mobile: (510) 681-6638