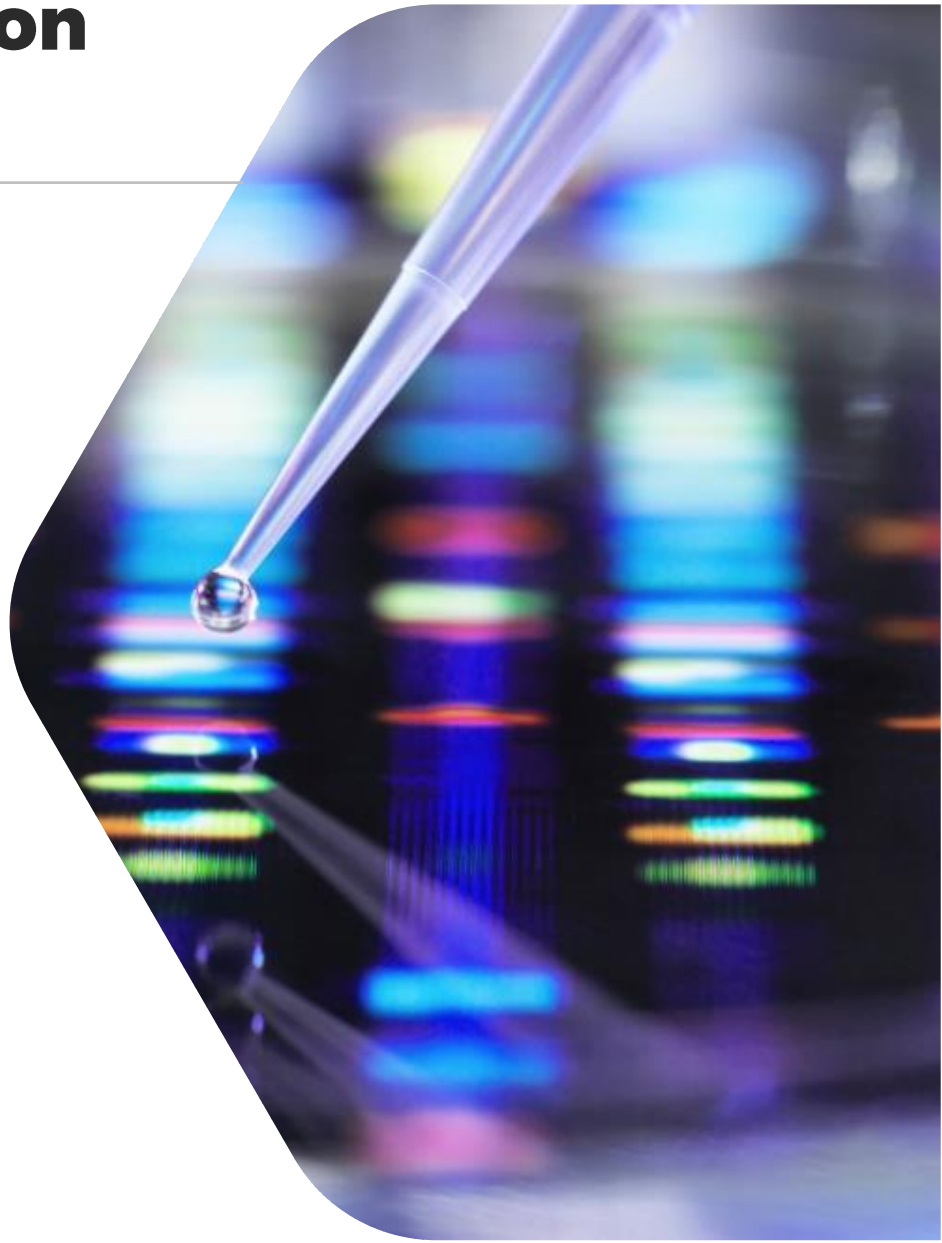
# Statement on Standards for Attestation Engagement (SSAE) 18

- This is a U.S. auditing standard issued by the American Institute of Certified Public Accountants (AIPCA)
- It addresses engagements undertaken by a service auditor for reporting on controls at service organizations



# Statement on Standards for Attestation Engagement (SSAE) 18

- It applies to entities that provide services to users, for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting
- The SSAE 18 standard is used to produce three types of System and Organization Controls (SOC) reports - SOC 1, 2 and 3

# Service Organization Control (SOC)

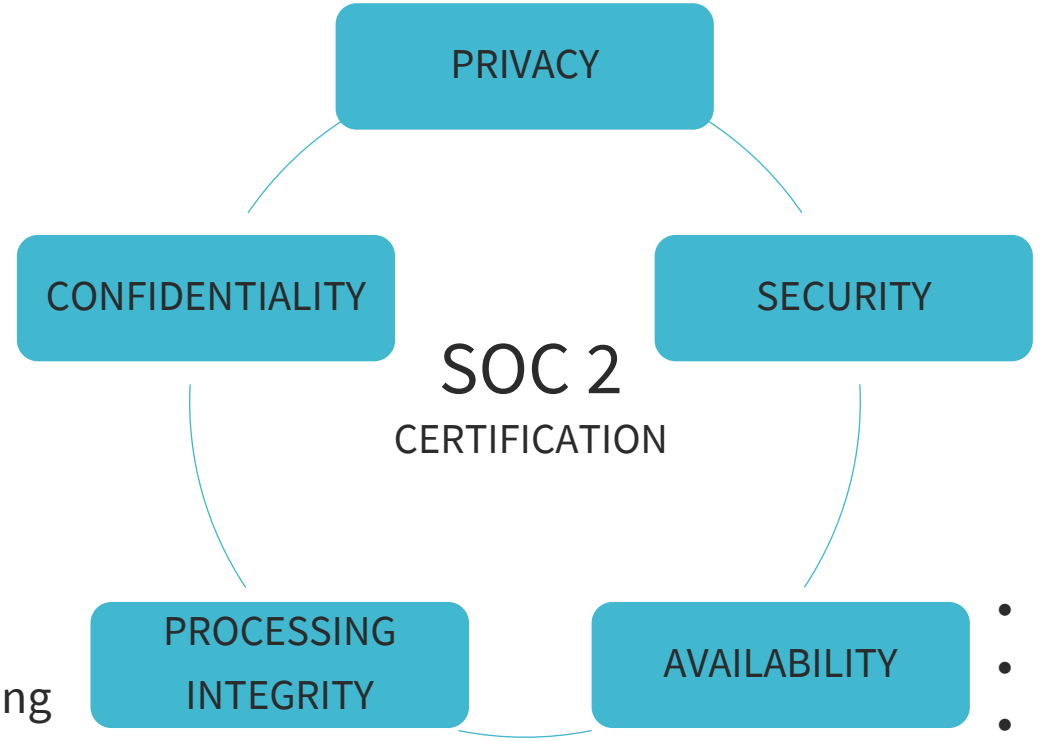
- Information security is of particular for concern for enterprises outsource critical business operation to third-party vendors such as SaaS providers
- Mishandled data, especially by application and network security providers, can leave organizations vulnerable to data theft, extortion and ransomware installation
- SOC 2 is an auditing technique that helps service providers securely manage customer data and safeguard the interests and privacy of organizations

# Service Organization Control (SOC)

- SOC 2 compliance is a minimal requirement when considering a SaaS provider
- SOC 2 defines criteria for managing customer data based on five “trust service principles”—security, availability, processing integrity, confidentiality and privacy

# SOC 2

- Access control
- Two-factor authentication
- Encryption




- Encryption
- Access controls
- Network/application firewalls

- Network/application firewalls
- Two-factor authentication
- Intrusion detection

- Quality assurance
- Processing monitering

- performance monitoring
- Disaster recovery
- Security incident handling

# Internal Information Security Management System (ISMS)

- An Information Security Management System defines and demonstrates an organization's approach to information security and privacy
- It assists in the identification and assessment of the threats and opportunities to information and any related assets
- ISMS protects the enterprise from data breaches and defends against the resulting disruptions

# Internal Information Security Management System (ISMS)

- ISMS assists you in winning new business from competitors and entering new sectors
- Strengthens your relationship with your existing customers
- Enables the building of your organization's brand and reputation
- Protects your business from security breaches

# Gap Analysis and Internal Information Security Management System

- The compliance security test and evaluation (ST&E) will review the operational plan (or planned implementation) of appropriate controls
- Tests conducted will include assessments, audits, security reviews, vulnerability scanning, and penetration testing
- Results are a risk assessment report that represents a **gap analysis**, documenting the system, application, or data risk

# Gap Analysis and Internal Information Security Management System

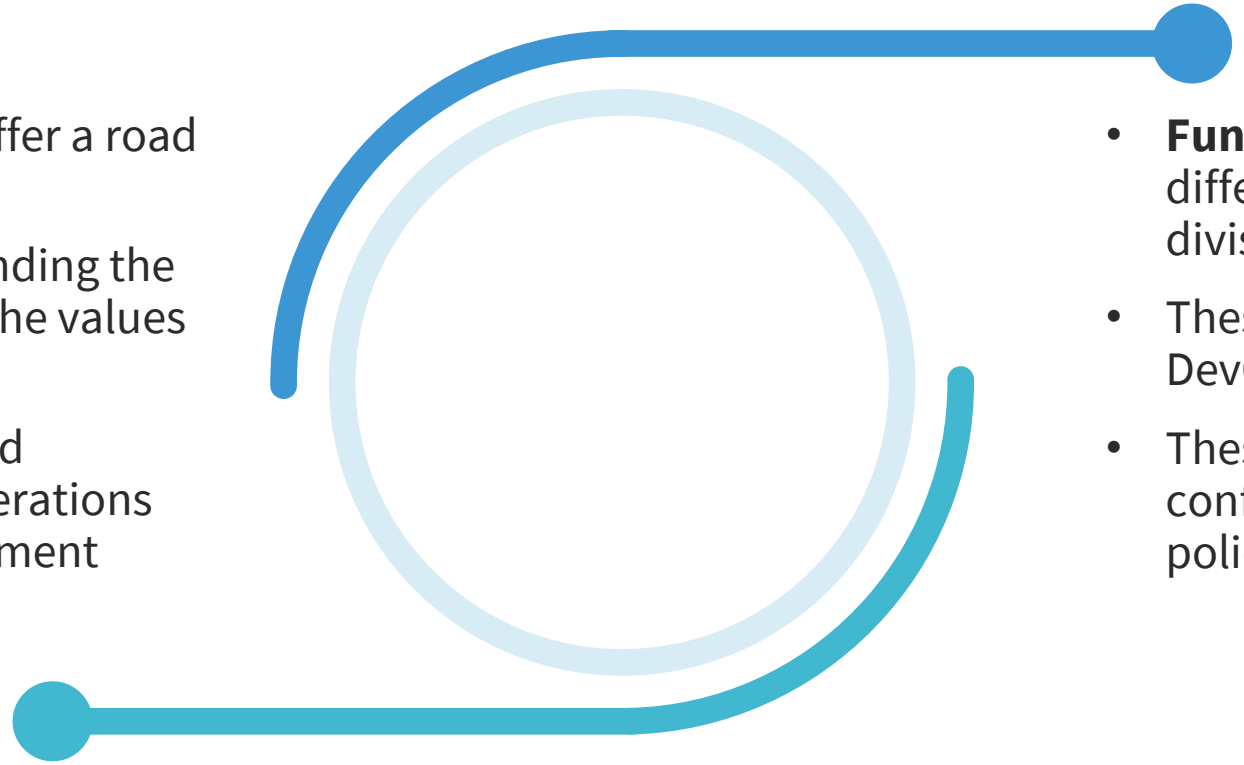
- The key first step to improving your organization’s security and compliance would be using NIST SP 800-171, ITAR, and other critical security focused standards
- The International Traffic in Arms Regulations (ITAR) is a US regulation that controls the export and import of defense articles and services on the United States Munitions List (USML)
- To fully understand where you are right now and what needs to change to meet your goals and the laws you are required to comply with

# IS Security Management with ITIL 4

- The new ITIL 4 Service Value System (SVS) describes the chain of activities necessary to convert a business opportunity or demand for a service into business value
- The IT service lifecycle has been refined into the Service Value Chain that acts as the core component of the SVS
- These components reflect the ITIL 4 focus on “the co-creation of value” and continual improvement

# Organizational vs. Functional Policies

- **Organizational** Policies offer a road map for daily operations
- They assist with understanding the organization's views and the values of specific issues
- Organizational policies and procedures help guide operations without constant management intervention



- **Functional** policies apply to different business units and divisions
- These range from financial, DevOps, marketing, and others
- These policies should never conflict with organizational policies

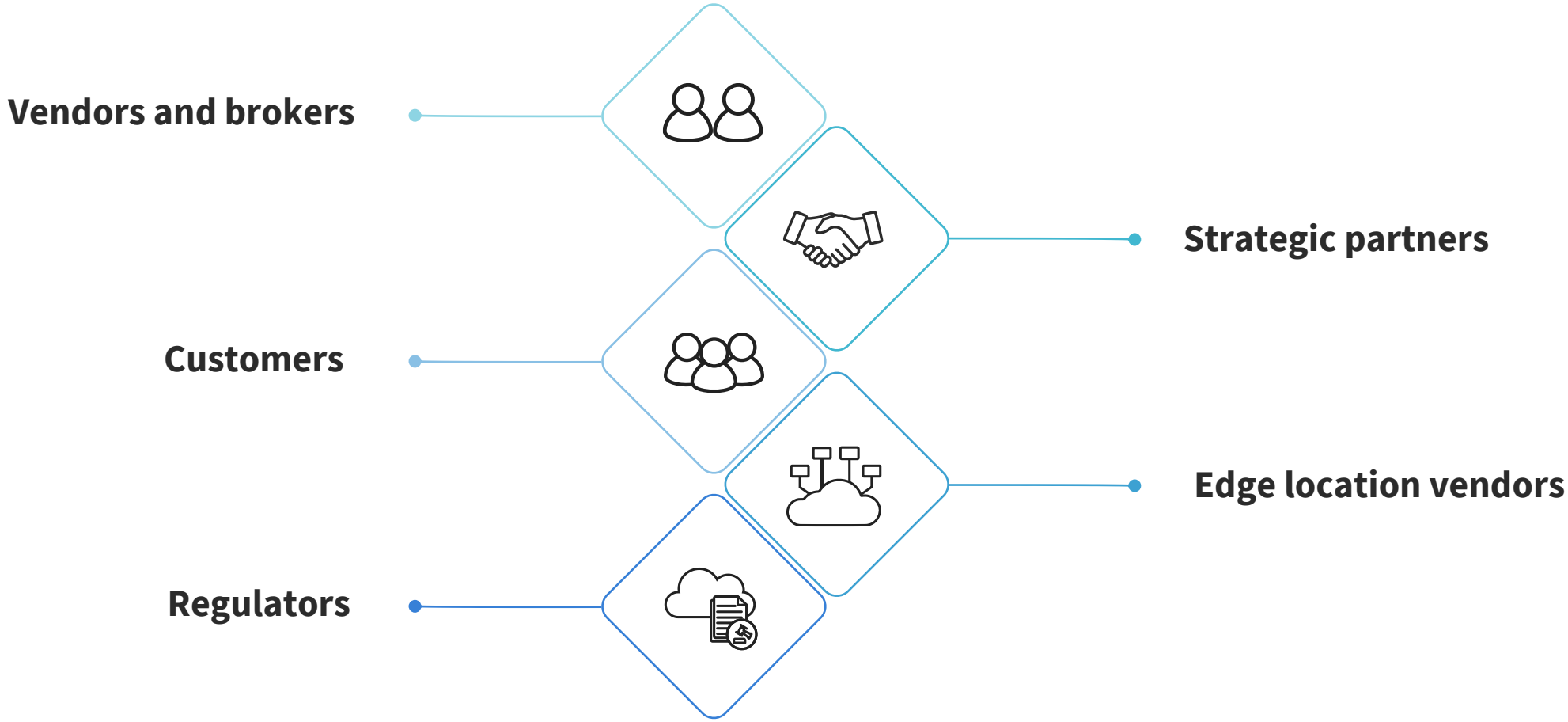
# RACI Charts for Mapping Stakeholder Roles

**R -** Responsible **A -** Accountable **C –** Consulted **I –** Informed

| | GRC* Department | Legal Department | Security Team | IT Operations |
|---|---|---|---|---|
| Establish the provider requirements | R/A | C | C | I |
| Build the governance scheme | R/A | C | C | I |
| Assess cloud vendor | A | I | R | R |
| Build the architecture | I | I | A/R | R |
| Conduct cloud migration | I | I | C | A/R |

*GRC – Governance, Risk, and Compliance

# Cloud Computing Stakeholders

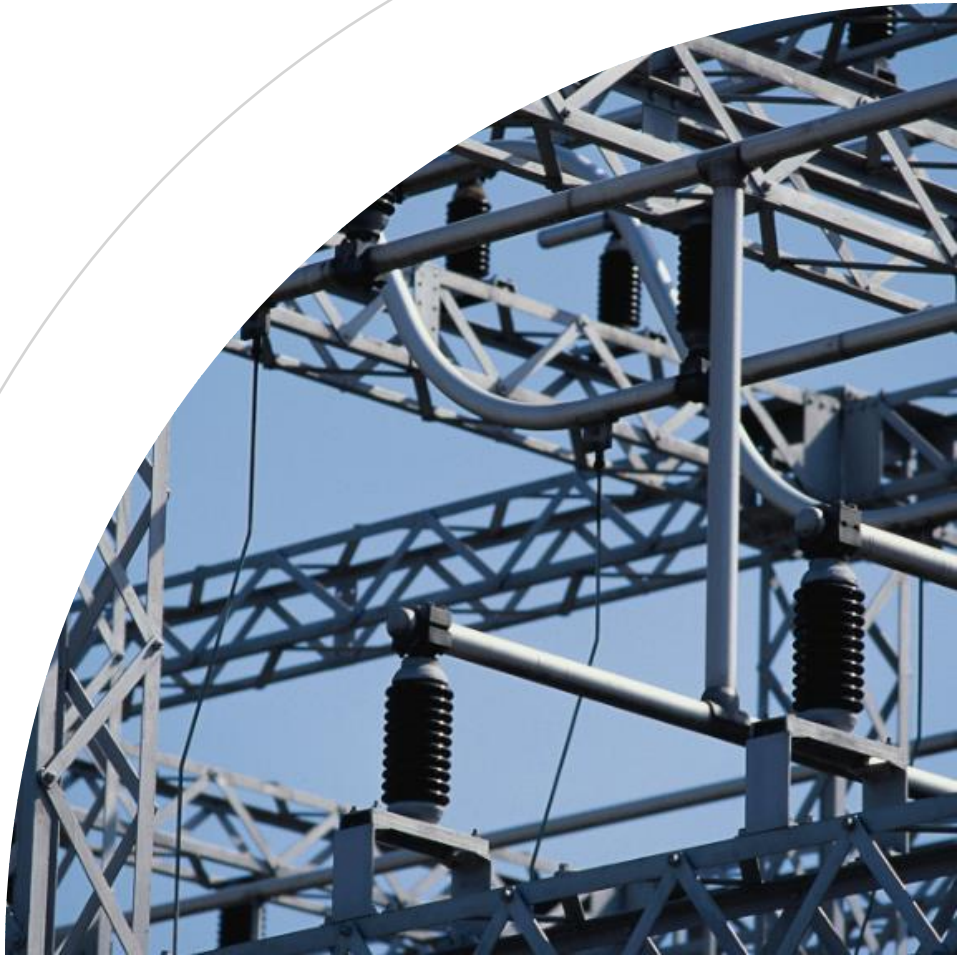


# Highly Regulated Industries: NERC/CIP

- To fortify the cyber resilience of the US, the government created the North American Electric Reliability Corporation (NERC) framework  designed to protect a part of the utility infrastructure of the US
- The NERC Critical Infrastructure Protection (CIP) Standards apply specifically to the cybersecurity aspects of the Bulk Electric System and its efficient and reliable supply
- CIP deals with the pre-planning and groundwork within organizations and agencies to tackle threats to the effective and timely functioning of national and regional critical infrastructure

# 10 Areas of NERC/CIP

1. Identification and Categorization
2. Security Controls
3. Background Checks and Training
4. Electronic Security
5. Physical Security
6. System Security
7. Incident Management
8. Recovery Plans
9. Configuration and Vulnerabilities
10. Information Protection



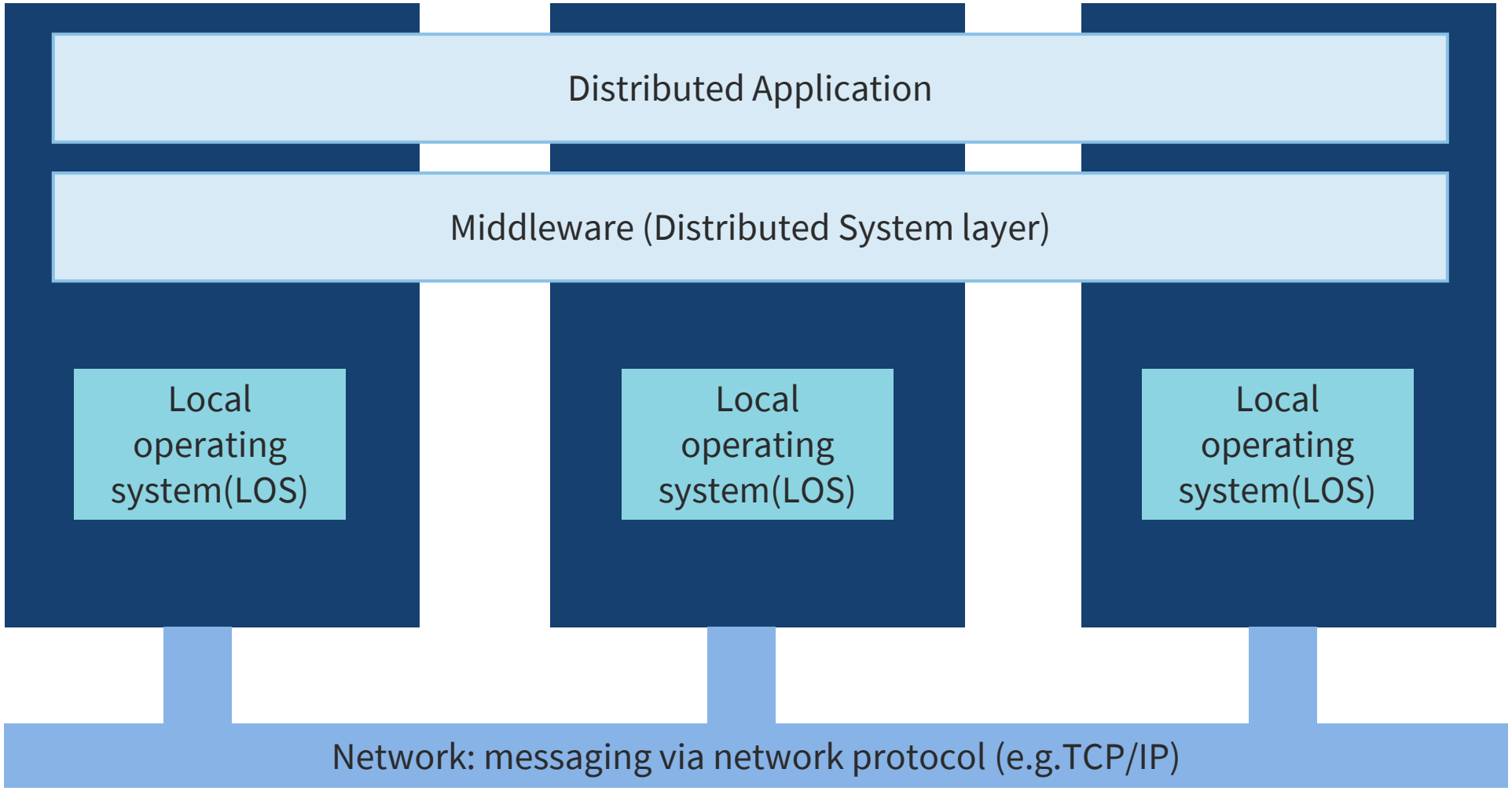
# Highly Regulated Industries: HIPAA/HITECH

- HIPAA predates the HITECH Act by 13 years and is concerned with the portability of health insurance (ensuring employees do not lose coverage while between jobs), and the privacy and security of health data
- The HITECH Act updated HIPAA and is concerned with promoting the adoption of electronic health records and meaningful use of health information technology and is part of the American Recovery and Reinvestment Act of 2009


# Highly Regulated Industries: PCI

- The Payment Card Industry Data Security Standard (PCI DSS) security standards were formed in 2004 to secure credit and debit card transactions against data theft and fraud
- While the PCI SSC has no legal authority to compel compliance, it is a requirement for any business that processes card transactions
- PCI certification is also considered the best way to safeguard sensitive data and information

# Challenges to Distributed Cloud Applications



# Business Agreement Requirements: SLA

- The CSP must realize that the use of contractual agreements such as hosting/connection agreements and Service Level Agreements (SLAs) are used to allocate shared responsibility and risk among both cloud providers and cloud consumers
- An SLA defines the precise responsibilities of the provider and sets customer expectations

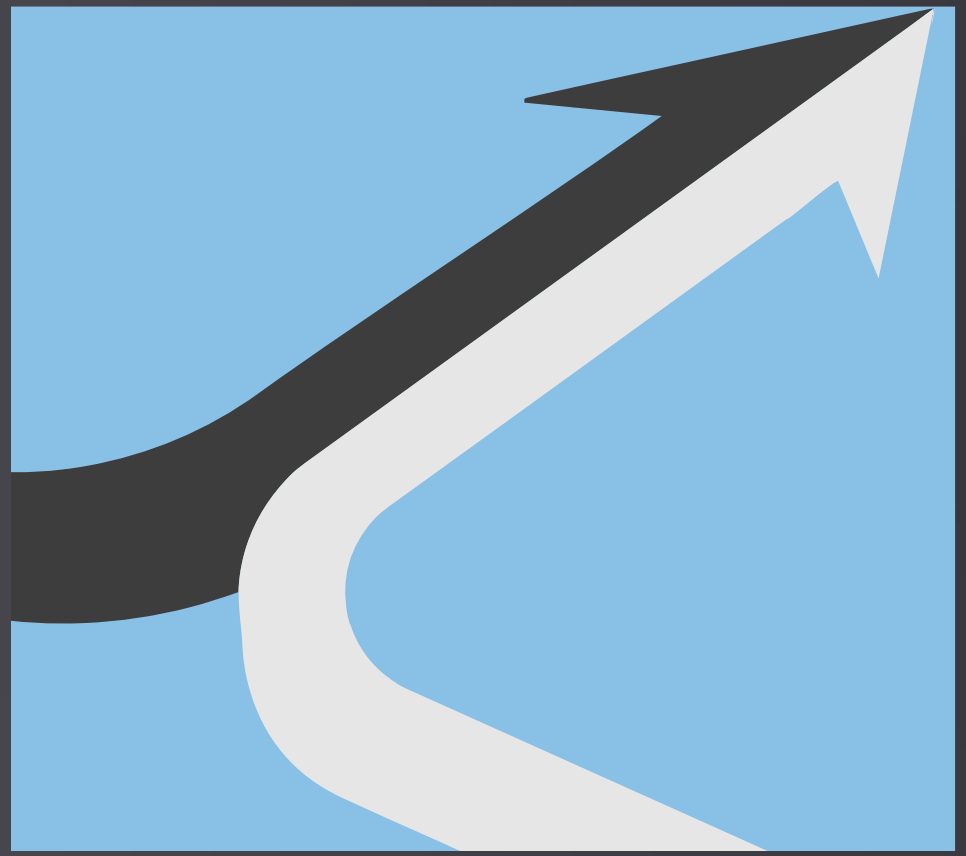
# Business Agreement Requirements: SLA

- Also clarifies the support system (service desk) response to problems or outages for an agreed level of service (based on support plan)
- The liability for the failure of one or more controls and the realization of risk can be appropriately documented and understood by all involved parties

# Master Services Agreement (MSA)

- The SLA is also called a Master Service Agreement (MSA)
- A master service agreement (MSA) is a contract two parties enter into during a service transaction
- This agreement details the expectations of both parties
- The goal of a master service agreement is to make the contract process faster
- It also should make future contract agreements simple

# Elements of SLA and MSA



Confidentiality

Delivery requirements

Dispute resolution and liability limits

Geographic locations

Intellectual property rights

Payment terms

Venue of law

Warranties

Work standards

# Statement of Work (SOW)

- An agreement that establishes the expectations for a project or program and aligning the team(s) involved
- Details should clarify price, cost, timeline, deliverables, process, expectations of requirements, invoicing schedules, and much more, depending on the scope and breadth of the project

# Statement of Work (SOW)

- Basically, a SoW is a document of agreement between a client and service or agent defining the scope and details of a project
- It is among the first documents you will use to establish the framework of a project before entering the planning and execution stages

# Vendor Management: Benchmarks

- Benchmarks are a technique to improve an organization's information security management by establishing a standard
- CIS Benchmarks™ are best practices to securely configure various systems and are available for more than 140 technologies

# Vendor Management: Benchmarks

- Established using a special method constructed from an accord of global cybersecurity experts from across the globe
- CIS Benchmarks™ are security configuration guides created by government, business, industry, and academia

# CSA Cloud Controls Matrix (CCM) and the Consensus Assessment Initiative Questionnaire (CAIQ)

- The CCM is 197 control objectives structured in 17 domains covering all key aspects of cloud technology
- Often used for the systematic assessment of a cloud implementation
- Offers guidance on which security controls should be implemented by which actor within the cloud supply chain
- It is considered the de-facto standard for cloud security assurance and compliance
- The STAR Level 1: Security Questionnaire (CAIQ v4) offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services

# CSA CCM Domains

- Application & Interface Security (AIS)
- Audit Assurance & Compliance (AAC)
- Business Continuity Management & Operational Resilience (BCR)
- Change Control & Configuration Management (CCC)
- Data Security & Information Lifecycle Management (DSI)
- Datacenter Security (DCS)
- Encryption & Key Managemnt (EKM)
- Governance & Risk Management (GRM)
- Human Resources (HRS)
- Identity & Access Management (IAM)
- Infrastructure & Virtualization Security (IVS)
- Interoperability & Portability (IPY)
- Mobile Security (MOS)
- Security Incident Management, E-Discovery, & Cloud Forensics (SEF)
- Supply Chain Management, Transparency, and Accountability (STA)
- Threat & Vulnerability Management

# Supply-chain Management (ISO/IEC 27036)

- ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information risks involved in the acquisition of goods and services from suppliers

# (ISO/IEC 27036)

- The implied context is business-to-business relationships, rather than retailing, and information-related products
- The terms acquisition and acquirer are used rather than purchase and purchasing since the process, information risks and controls are much the same whether the transactions are commercial or not