

# CYBER SECURITY & CLOUD COMPUTING - CONCEPTS, CHALLENGES AND OPPORTUNITIES FOR CHARTERED ACCOUNTANTS

CA Sanjay Anant Deshpande



# AGENDA

- What is Cyber Security ?
- What is Cloud Computing?
- Why Cloud ? Key Benefits
- Key Market Players
- Threats
- Challenges
- Opportunities
- Examples of control testing
- Introduction to Technical terms
- IT Domains



# Cybersecurity & IS

**Cyber** : Kubernetes → Cybernetics

**Cybersecurity**: protecting electronic devices and associated data and information.

**Information Security (IS)**: protecting CIA triade

At NIST, one definition in use is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its **availability, integrity, authentication, confidentiality, and nonrepudiation**. This comes from a Glossary on the NIST website: :

<https://csrc.nist.gov/Glossary/?term=3817#AlphaIndexDiv>



# Cloud Computing- Characteristics

Broad Network Access

On Demand Service

Measured Service

Resource Pooling

Rapid Elasticity

+ Shared Tenancy

**NIST SP 800-145** provides a one sentence definition of **cloud computing** as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”





# Key Benefits

Economy

Agility

Resiliency



# Key Players

**AWS**-Amazon Web Services by Amazon (34%)

**Azure**-Microsoft (18%)

**GCP**-Google Cloud Platform

**Oracle Cloud**

**IBM**

490 US Billion Dollars in 2022 (expected 590 in 2023)



# Cyber Attack Types

- Malware Attacks
- Phishing Attacks / Social Engineering Attack
- Password Attacks
- Man-in-the-Middle: Eavesdropping
- SQL Injection Attacks
- Denial-of-Service Attacks
- Inside Threat (espionage,theft,sabotage)
- Zero-Day-Exploit



# Cyber Attack incidences

- **Stuxnet:** 2010- Iran's nuclear centrifuge blown up
- **Log4J:** Nov.2021-Execute malicious code remotely
- **Solar Wind:** 2019-Orion Supply Chain attack-  
malicious code injected thru n/w monitoring tool
- **Solar Industries Nagpur:** 2023-2TB data stolen-  
contract with army and other suppliers,  
engineering drawings etc. compromised





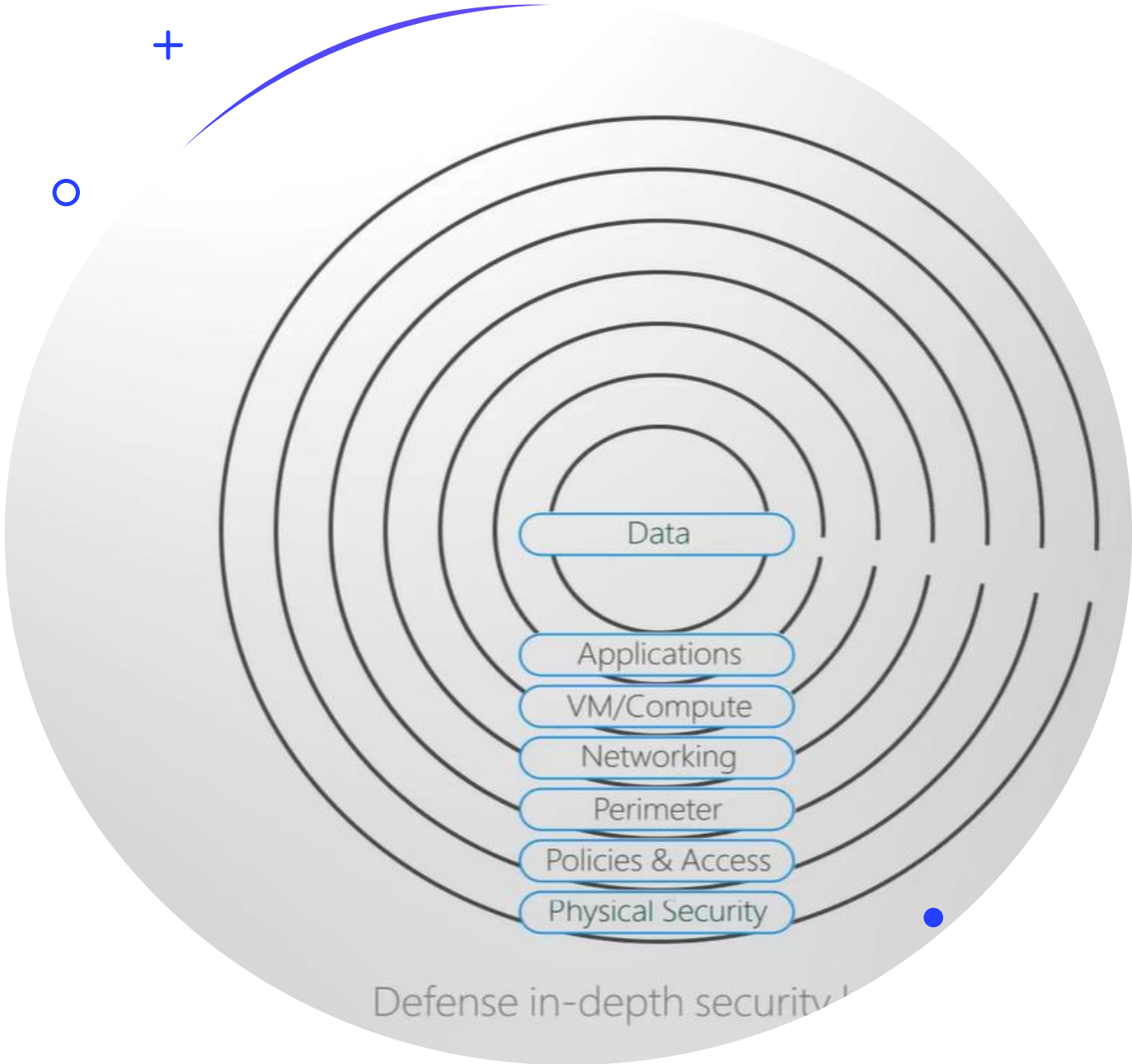
# OWASP Top Ten

## Open **W**eb **A**pplication **S**ecurity **P**roject

1. **Broken Access Control**
2. **Cryptography Failure**
3. **SQL Injection**
4. **Security Misconfiguration**
5. **Insecure Software Design**
6. **Identity and Authorization Failure**
7. **Vulnerability and outdated components**
8. **Monitoring and Logging Failure**
9. **Software and Data Integrity Failure**
10. **SSRF-Server-Side Request Forgery**



# Defence-in-depth



- Source: Azure

# Cloud Governance Risks & Challenges

- Loss of direct control over Infrastructure**
- Data may span over multiple jurisdictions**
- Visibility and transparency in cloud service is challenging**
- Ownership is still with Org**
- Service offerings may be inflexible**
- CSPs vary in level of maturity**
- Supply Chain makes scoping challenging**
- Shared responsibilities**
- Hybrid model makes difficult to know boundaries**
- Reliance is more on assessments than experiential tests**
- Rapid changes in cloud technology**



# Opportunities

Gartner predicts that through 2025, **more than 99% of cloud breaches will be traced back to preventable misconfigurations or mistakes by end users.** Gartner's latest Hype Cycle for Cloud Security report reflects the progression enterprises are making in adopting cloud-first strategies across all lines of business and at the infrastructure level.

- Conduct Cybersecurity Audit mandated by RBI,IRDAI,SEBI
- SOC 2 audits (ISAE 3402 and ISAE 3000)
- Internal Audit
- Consulting Services : examples
  - ✓ Governance Policy
  - ✓ Information Security Policy
  - ✓ Password Policy
  - ✓ Data Privacy, Retention and Disposal Policy
  - ✓ Change Control Policy
  - ✓ Incident Response Policy
  - ✓ Standard Operating Procedures
  - ✓ Guidelines
  - ✓ IT Risk Evaluation / Assessment and Management



# What and how you can help ? Things to keep in mind:

## **IT Security concerns - Senior Management's perspective:**

- Assets security - Applications, Programs, H/W, S/W, People etc.
- Risk Assessment and Management – 6 kinds of risks
- Controls Design
- Controls Effectiveness
- IT Architecture security (Blast Radius, DMZ, Redundancies, Gateways, Ports, Firewalls)
- Data Life Cycle security (create, store, process, share, archive, destruct)
- N/W security - Firewalls ACLs, **Intrusion Detection System** and **Intrusion Prevention System**, Honey Traps
- S/W security
- Inventory of legal and authorized s/w
- Prevent unauthorized s/w installations
- Patching – servers, d/b, apps (log4j, solarwinds)
- Employee Training – Phishing attacks
- Access to development and production environment
- Back up procedures – BCP and DRP drills
- Robustness of onboarding process – employees, vendors
- Logging and monitoring

+





# What and how you can help ? Things to keep in mind:

- ❑ **Cloud adoption criteria:** Org goals for which it is accountable are met. **Assurance**, Trust(**B**elief-**E**xpectancy-**W**illingness to take Risk), and **A**ccountability of CSP.
- ❑ **Contract of adhesion**
- ❑ **SLAs:** 6 components
- ❑ **Ways to establish Cloud Trust:** Due Diligence: Supply Chain intelligence, STAR program, Sandbox, Secondary sources, Reported incidents, Desktop reviews
- ❑ **Org Systems** that drive measures : Ri-G-I-D
- ❑ **5 COSO Principles**
- ❑ **Who is responsible** for measures/controls: GRC team, Legal, Procurement and IT Operations
- ❑ **Compliance Team task to:** Validate that **M**easures are **D**esigned and **O**perated as **I**ntended
- ❑ **TOD & TOE:** E.g. API-PR Interface
- ❑ **Vulnerabilities:** MASS
- ❑ **Threats model:** STRIDE
- ❑ **Risk Management:** MART
- ❑ **Performance Matrix :** EQUATOR
- ❑ **Monitoring & Reporting Process:** McGRAF

+



# Knowledge Base

**ISO** - International Organization for Standardization

27017,17788,17789,19086, 21878 → All Cloud specific standards

**SANS** Institute

**ISACA** – Information Systems Audit and Control Association

**NIST** – National Institute of Standards and Technology

**COSO**- Committee of Sponsoring Organizations of the Treadway Commission

**MITRE ATT@CK**

**CSA** – Cloud Security Alliance

**ENISA**-The European Union Agency for Cybersecurity

**BSA** C5: Cloud Computing Compliance Controls Catalog



# Change Control and Configuration Management

- ❑ Is there a well documented policy on Change Control & Configuration Management ? How often reviewed and approved ? Once or twice a year ?
- ❑ How service tickets are logged and processed ?
- ❑ How unauthorized changes are protected ?
- ❑ Changes e.g. One-Off Patch, Roll up Patch, Weekly Security Patches, Data Fixes, Interface, Application, Configuration change (set ups, lookup tables, user profiles etc.)
- ❑ Documentation e.g. Oracle's MD50, MD70, MD120 – Business Requirements, Impact Analysis, Risk Analysis, Mapping, Design document e.g Interface, Implementation roll out instructions for UNIX admins, DBA, Roll back procedure.
- ❑ Approval from development Peer Review, Security Review (SOD), QA (steps in testing scripts, bug logs, retesting), SMEs, Evidence of UAT and Regression Testing, Change Control Board etc.
- ❑ If change was due to security incidence - RCA
- ❑ How changes are communicated to stakeholders

+



# IAM – Identity and Access Management

- Is there a well documented policy on IAM ? How often reviewed and approved ? Once or twice a year ? How it is communicated ?
- Are strong password policies and procedures documented, approved, implemented, communicated ?
- Is system identity information and levels of access managed, stored, and reviewed ?
- Is SOD principles employed ? – **E.g. PR/PO, Invoice Approval / Payment, MFA & Alerts for logging by DBA**
- Is the least privilege principle employed ?
- Is a process in place to de-provision or modify the access, in a timely manner ?
- Are SODs and Least Privilege reviewed with frequency commensurate with org's risk tolerance ?
- Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period ?
- Are processes, procedures and technical measures to ensure the logging infrastructure is “read-only” for all with write access ?
- Are users are identifiable through unique identification ?
- Are processes, procedures and technical measures for authenticating access to systems, application and data assets including MFA for a least-privileged user and sensitive data access defined, implemented and evaluated ?

# Technical Terms

Cybersecurity

On-Premise vs Cloud

CSP and CSC

Deployment Models

Delivery Methods

Abstraction aka Virtualization

Automation aka Orchestration

DevOps and DevSecOps

Responsibility Matrix





# Components of Infrastructure

Controller	Compute	Network	Storage
1. API Server	Hypervisor	1. SDN *	1. Volume Mgmt
2. Message Que		2. DHCP **	2. Raw Storage
3. Database		3. Security Groups	

+



# Deployment Models

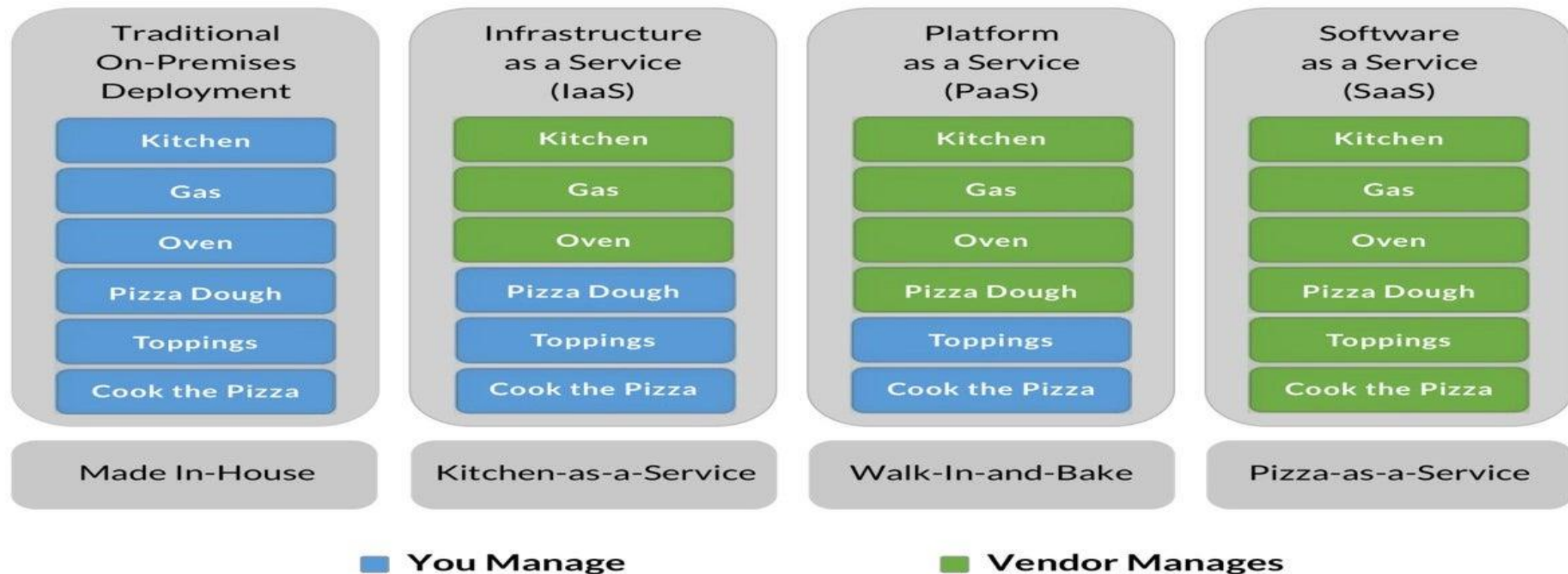
	Ownership	Management	Location	Trusted ?
Public	3 <sup>rd</sup> party	3 <sup>rd</sup> party	Off Premise	No
Private	Either 3 <sup>rd</sup> party or ORG	Either 3 <sup>rd</sup> party or ORG	Either Off Premise or On Premise	Yes
Community	Either 3 <sup>rd</sup> party or ORG	Either 3 <sup>rd</sup> party or ORG	Either Off Premise or On Premise	Yes
Hybrid	Both 3 <sup>rd</sup> party and ORG	Both 3 <sup>rd</sup> party and ORG	Both Off Premise and On Premise	Yes / No

+

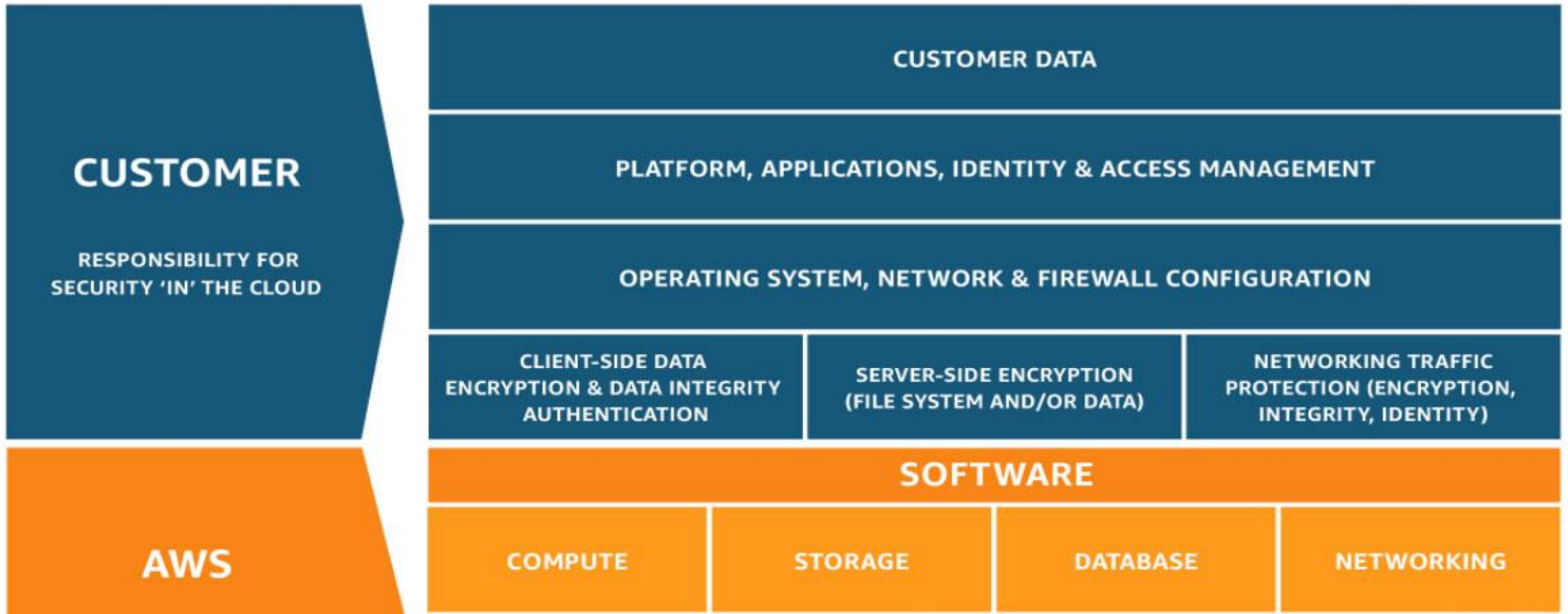


# On-Premise vs Cloud

## New Pizza as a Service




# Shared Responsibility Model



## IT LEADERSHIP POSITIONS

 Digital Adoption



**Chief  
Information  
Officer**




**Chief  
Technology  
Officer**



**Chief  
Information  
Security  
Officer**



**Chief Data  
Officer**



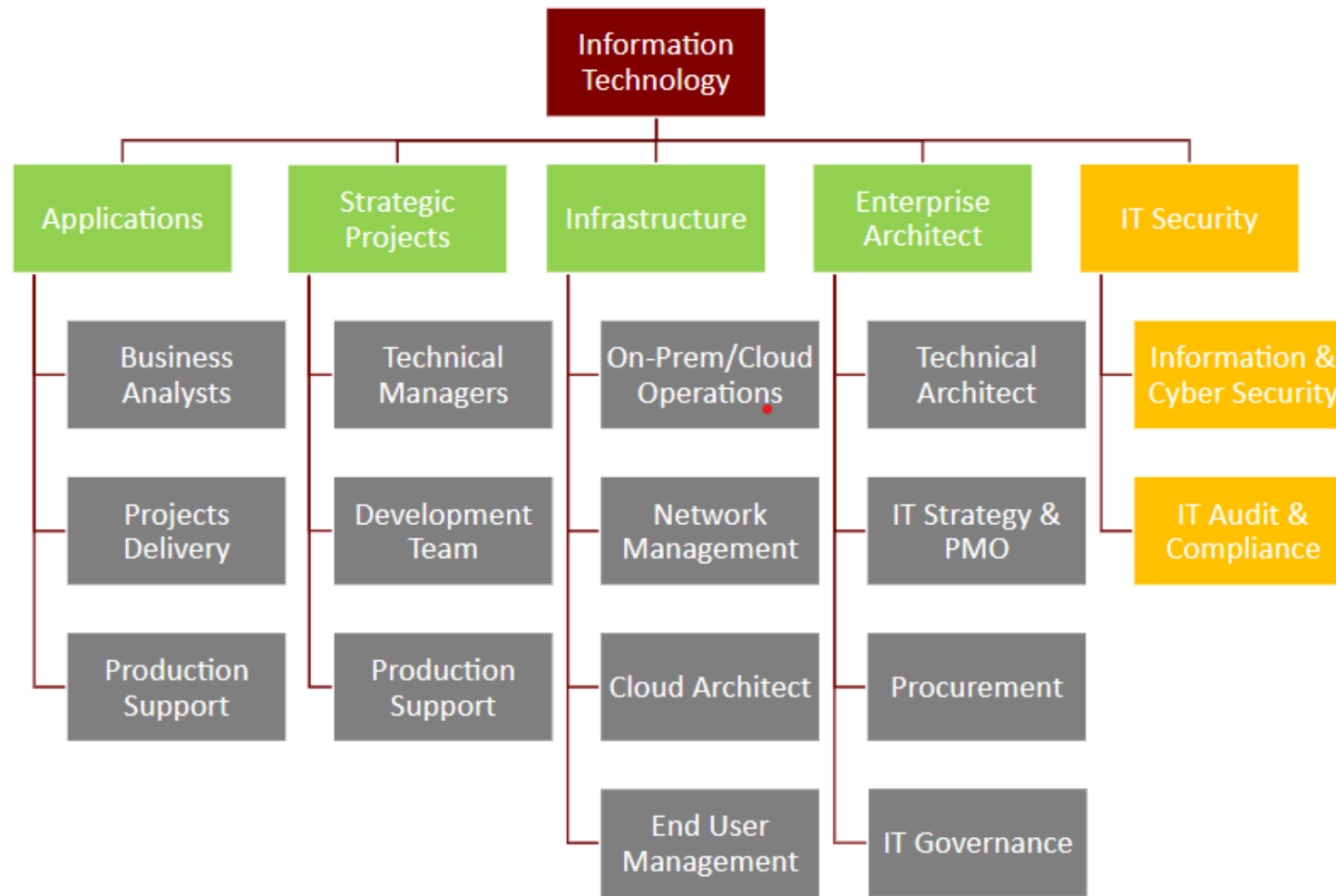
**Chief Digital  
Officer**

+

•



# IT organization hierarchy



# Controls

- **Internal Controls**
- **IT General Controls**
- **Application Controls**

**COBIT:** Common Objective for Internal Control – ISACA Framework

**COSO:** Committee of Sponsorship Org for Treadway Commission.  
Framework for evaluating control systems

**C5:** Cloud Computing Compliance Criteria Catalogue

**CCM:** Cloud Control Matrix

**ISO 27000 series:** Guidelines and Requirements

**IDRAI:** 17 IT domains – 307 control requirements

**RBI Cyber Security Framework** DBS/CO/CSITE/BC.11/33.01.001/2015-16  
dt June 2,2016

**SOX**

**SOC 1,2,3 Type I and II:** 5 TSCs - Trust Service Criteria



# GRC

## Governance, Risk and Compliance

**Governance:** Policies, Procedures and Controls are the pillars. Method by which stakeholders' needs are evaluated to determine if they are consistent and complimentary to achieve objectives to which org is accountable for.

**Risk:** Likelihood of THREAT exploiting VULNERABILITY causing damage/harm to org's assets.

**Threat :** Potential occurrence that may cause undesirable outcome

**Vulnerability:** Weakness, Flaw, Loophole, Susceptibility etc.

**Compliance:** Ability to adhere to requirements



# Abstraction

 aka Virtualization.

Technology that separates resources from underlying physical resources

# Automation

 aka Orchestration.

Technology that allows to rapidly provision and de-provision resources.



# CSA

**Cloud Security Alliance's published:**

- **Security Control Guidelines – how to do**
- **CCM-what to do**
- **STAR Program (Security, Trust, Assurance and Repository): Governance, Risk and Compliance program for Security and Privacy – STAR level 1,2,3 – GDPR code of conduct**

**Standards, Framework and Public Registry at the core.**

- Framework for managing risk in the cloud**
- Maps 35+ standards (PCIDSS,ISO 27001, NIST etc.)**
- Lingua Franca**
- Public Registry open for scrutiny**
- Guidance for CSC and CSP**
- Lists 17 IT domains and 197 controls**
- CAIQ: Consensus Assessment Initiative Questionnaire (310 questions)**





# Cloud Threats – Egregious 11

1. **Data Breaches**
2. **Misconfigurations and inadequate Change Controls**
3. **Lack of Cloud Security Architecture & Strategy**
4. **Inadequate IAM, Key Management**
5. **Account Hijacking**
6. **Inside Threat**
7. **Insecure Interfaces and APIs**
8. **Weak Control Plane**
9. **Metastructure and Applistructure failure**
10. **Limited Cloud usage visibility**
11. **Abuse and nefarious use of Cloud Services**



# Cloud Control Matrix

## CCM structure:

1. Control ID
2. Control Title
3. Control Domain
4. Control Specification
5. Control Applicability & Ownership (IaaS,PaaS,SaaS)
6. Architectural Relevance-DARMOVSSN (acronym)
7. Organizational Relevance -  
Cybersecurity,Development,Internal Audit, GRC, Legal,  
HR etc.
8. Mapping



# IT Domains

AIS	Application Interface and Security
AAC	Audit Assurance and Compliance
BCR	Business Continuity and Resiliency
CCC	Change Control and Configuration Management
DSC	Data Center Security
DSI	Data Security and Information Lifecycle Management
EKG	Encryption and Key Management
GRM	Governance & Risk Management
HRS	Human Resource Systems
IPY	Interoperability and Portability
IVS	Infrastructure and Virtualization
IAM	Identity Access Management
MOS	Mobile Security
SEF	Security Incident Management, E-discovery and Forensics
STA	Supply Chain Management, Transparency and Accountability
TVM	Threat and Vulnerability Management
LOG	Logging and Monitoring



+



o



.



# THANK YOU

CA Sanjay Anant Deshpande  
sanjay.deshpande04@gmail.com