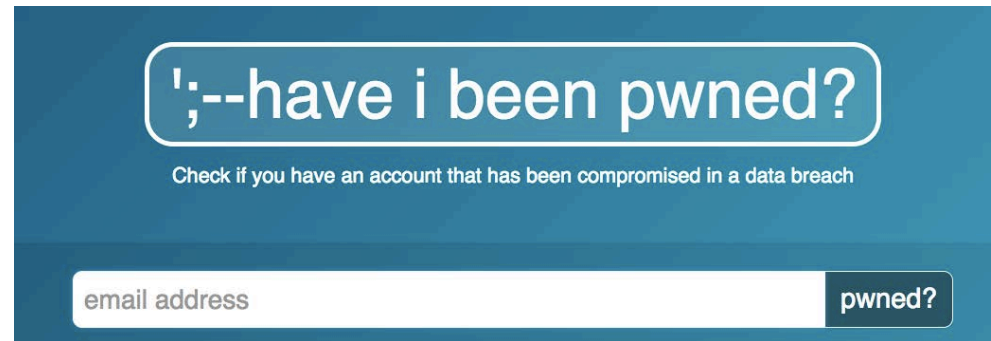


Cyberworld Security

June 23, 2018

Basic Security Test?



The image shows a screenshot of the 'have i been pwned?' website. The header features the text 'have i been pwned?' in a white, rounded box on a dark teal background. Below the header, there is a smaller line of text: 'Check if you have an account that has been compromised in a data breach'. At the bottom of the screenshot, there is a search bar with the placeholder text 'email address' and a button labeled 'pwned?'.

<https://haveibeenpwned.com/>


Cybersecurity Statistics

- Warren Buffet says that cybercrime is number one problem of mankind, bigger than nuclear weapons.
- Total cost of a Cybercrimes in 2021 - \$ 6 trillion. (more than the global trade of drugs).
- Cybersecurity spend - \$96 Billion in 2018, to reach \$ 1 trillion in 2021.
- Global Ransomware alone cost \$5 billion.


Cybersecurity Breach # 1 (Mossack Fonseca)



Network Segmentation

- Network Segmentation Policy (Documented)
- VPC/VNET
- Dedicated connectivity with on-prem (expressroute/Directconnect/Cloud Interconnect) 
- Outbound Internet access through gateway

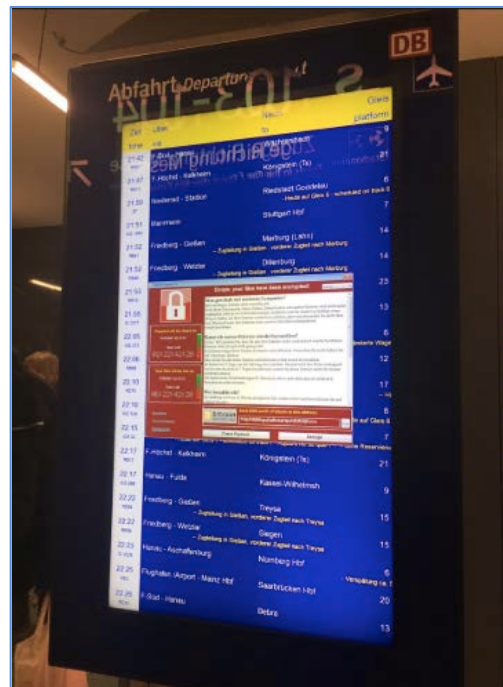
Server Security Assessments

- Vulnerability assessments and Patch Management
- Secure storage configuration (S3/Blob)
- Minimum baseline security standards (MBSS)
- Penetration testing 

Cybersecurity Breach #2 (Ransomware/Crypto mining)



Advertising Boards



Airport Displays



ATM's

Server Security Assessments

- Vulnerability assessments and Patch Management
- Secure storage configuration (S3/Blob)
- Minimum baseline security standards (MBSS)
- Penetration testing



Cybersecurity Breach #3 (Nationstate - Sony)

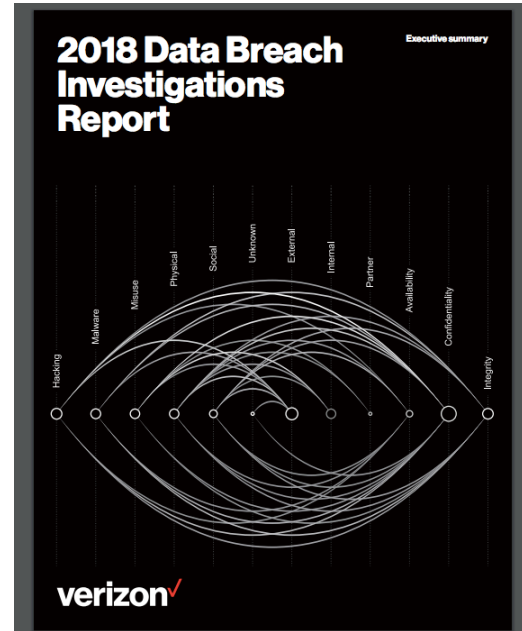


“We cannot have a society in which some dictators someplace can start imposing censorship here in the United States because if somebody is able to intimidate us out of releasing a satirical movie, imagine what they start doing once they see a documentary that they don't like or news reports that they don't like.”

Cybersecurity Breach #4 (Zomato)



Verizon data breach report

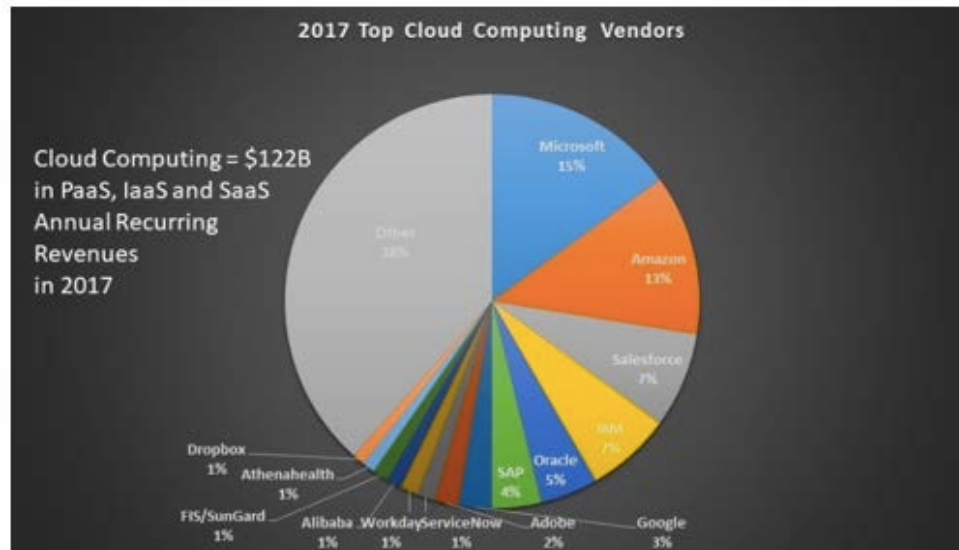


Hybrid Cloud Security

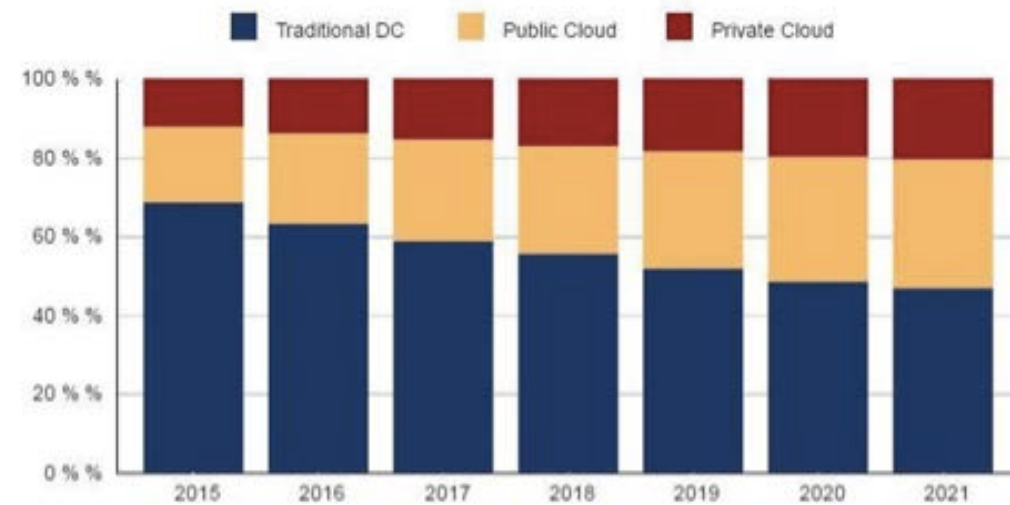
June 23, 2018

Why Cloud Computing?

- Cloud Computing Market to grow to **\$162 Bn** in 2020 from **\$67 Bn** in 2015 (CAGR 19%).
- By 2021, more than half of the global enterprises using cloud today will adopt an all-in cloud strategy; Increased adoption in India after presence of big 4 – AWS, Azure, IBM and Google.



Worldwide Cloud IT Infrastructure Market Forecast by Deployment Type 2015 - 2021 (shares based on Value)

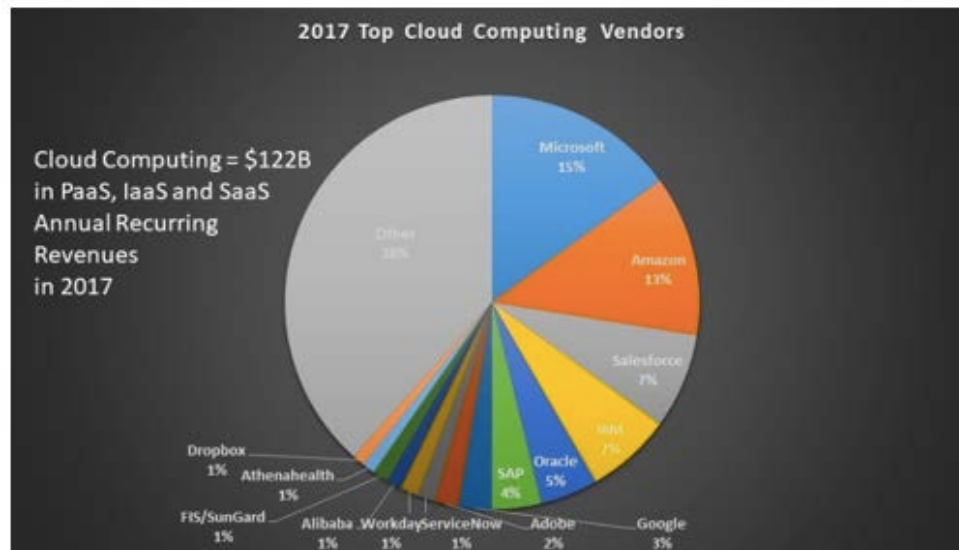


Source: IDC

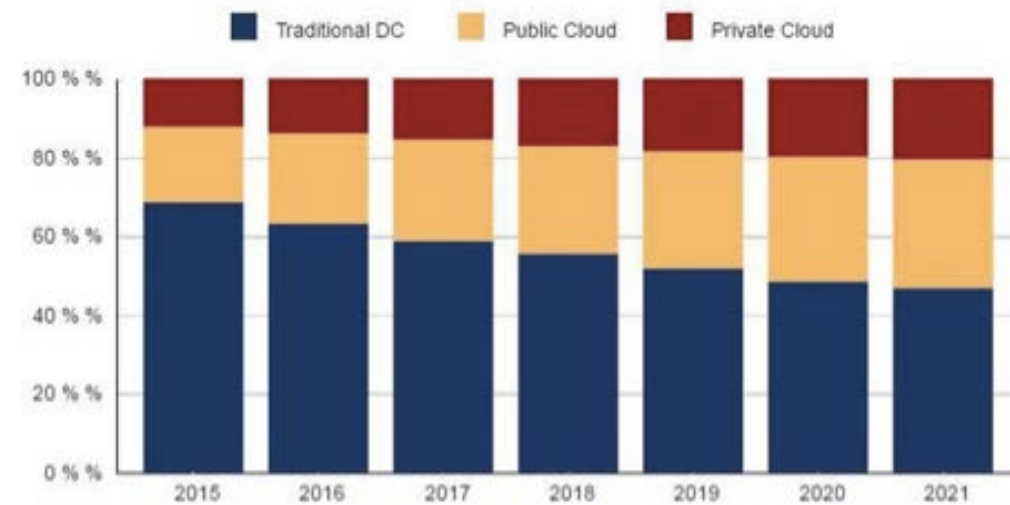
Why Cloud Computing?

Popular with Start-ups:

- SMB/Small Companies can have all the desired resources within hours, if not, minutes.
- No or little upfront cost.
- Don't need manpower for infrastructure management.



Worldwide Cloud IT Infrastructure Market Forecast by Deployment Type 2015 - 2021 (shares based on Value)

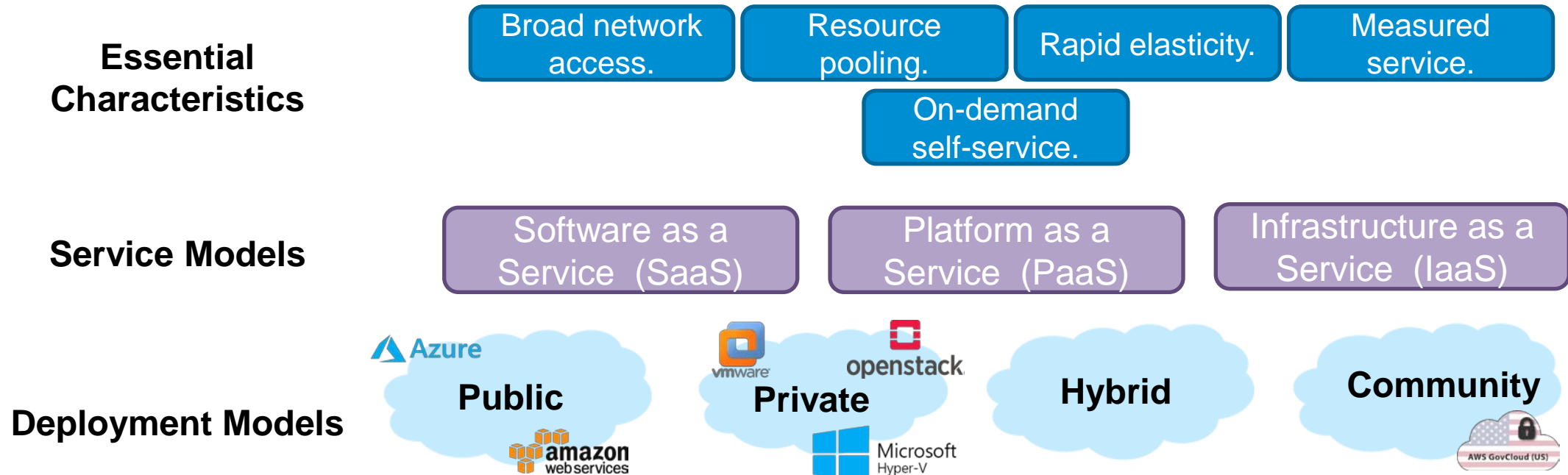


Source: IDC

What is Cloud?

Cloud computing is a model for enabling ubiquitous, convenient, *on-demand network* access to a *shared pool of configurable computing resources* (e.g., networks, servers, storage, applications, and services) that can be *rapidly provisioned and released with minimal management effort* or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

SP 800-145, The NIST Definition of Cloud Computing

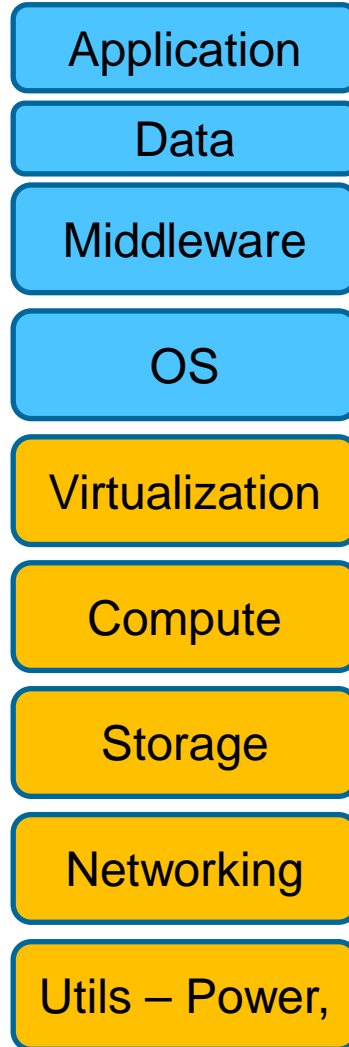


Service Models - Details

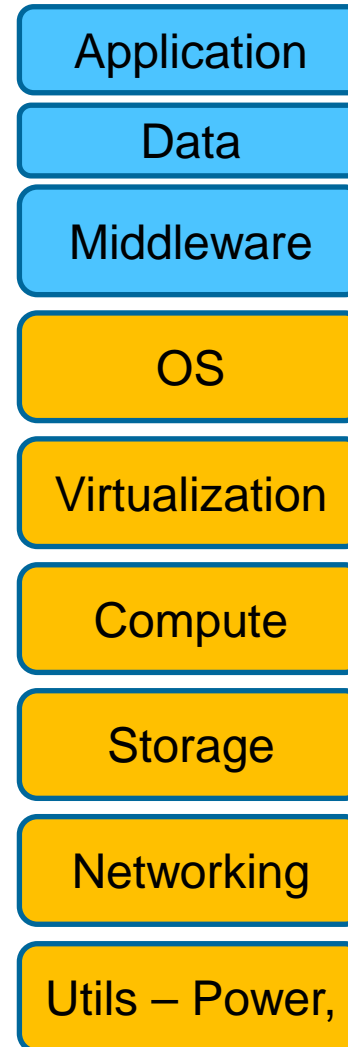
On-Premises



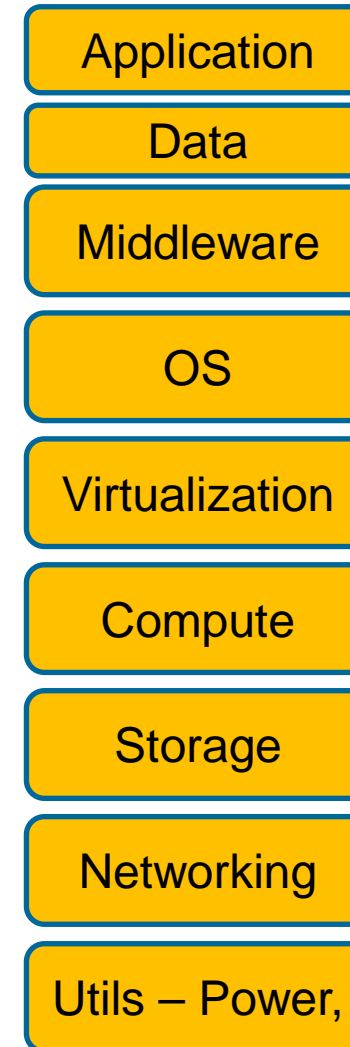
IaaS



PaaS



SaaS



Managed
by
Provider

Managed
by
You

Public Clouds : Shared Security Model

Responsibility	On-Premises	IaaS	PaaS	SaaS
Data classification, and security	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
End point security	Cloud Customer	Cloud Customer	Cloud Customer	Shared
Identity and Access Management	Cloud Customer	Cloud Customer	Shared	Shared
Application Security	Cloud Customer	Cloud Customer	Shared	Cloud Provider
Network Security	Cloud Customer	Shared	Cloud Provider	Cloud Provider
Host/Server Security	Cloud Customer	Shared	Cloud Provider	Cloud Provider
Physical Security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend:
Cloud Customer (Blue)
Cloud Provider (Yellow)

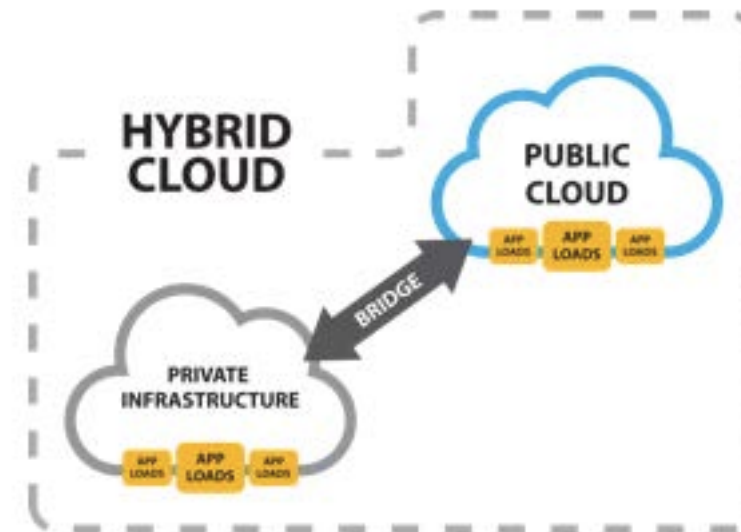
Source: Microsoft MSDN

Hybrid Cloud

Hybrid cloud is a cloud computing strategy, whereby an enterprise employs a combination of cloud environments – most usually public and private cloud, but it may incorporate any combination of virtualised, colocated or on-premises infrastructure – with orchestration between them.

Use Cases:

- **Light:** On-premises dedicated servers for the hosting of sensitive workloads, with non-critical workloads hosted with a public cloud provider.
- New projects/POCs on workloads in public cloud with existing production systems as-is in On-Prem.
- **Medium:** Test/Development hosted on a public cloud and production workloads in On-premises datacentre.
- **Heavy:** All workloads in public cloud and systems with sensitive information (regulatory) on workloads in On-Prem data centre.
- Most suitable for organisations, which use it to dip its toes into the cloud waters.



Hybrid Cloud - Advantages

- Most suitable path for the enterprises to harness the advantages of the cloud, without giving up existing enterprise data centers.
- Organizations do not want to be left behind.
- Advantages and benefits:
 - Capacity Augmentation.
 - Workload Portability.
 - Geo-Resiliency.
 - Achieve speed and scale for smaller teams/POCs.
 - New workloads on the cloud.

Cloud Security



CSA

Find compliance offerings

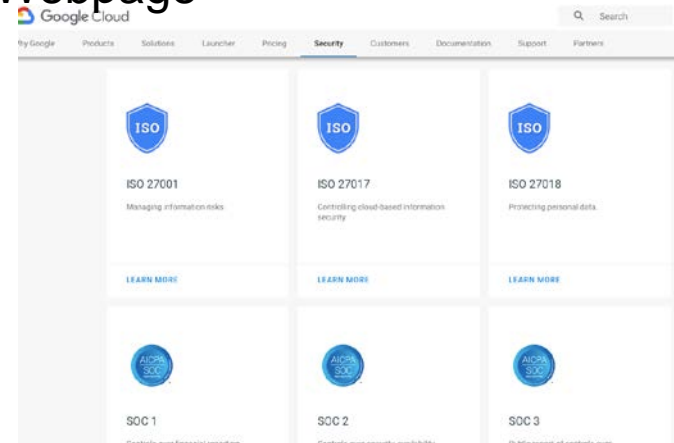
Global: Select one | Industry: Select one | Product or Service: Select one | Clear all

Global	US Government	Industry	Regional
CSA-STAR-Attestation	CIIS	23 NYCRR Part 500	BR 2012 (Netherlands)
CSA-STAR-Certification	DoD DISA L2, L4, L5	APIRA (Australia)	CS (Germany)
CSA-STAR-Self Assessment	DoE 10 CFR Part 810	CDSA	CCS/IRAP (Australia)
DFARS	EAR (US Export Administration Regulations)	DPF (UK)	CS Gold Mark (Japan)
ISO 20000-1:2011	FDA CFR Title 21 Part 11	FACT (UK)	Cyber Essentials Plus (UK)
ISO 22301	FeuRAMP	FCA (UK)	D/CP (China)
ISO 27001	FERPA	FFIEC	EN 301 549 (EU)
ISO 27017	RIPS 140-2	FSC (Japan)	ENISA IAF (EU)

Azure Security Compliance Webpage



AWS Security Compliance Webpage



Google Cloud Security Compliance Webpage

Hybrid Cloud - Solutions



AWS SnowMobile



Azure Cloud in a Box

EMC²
Federation Hybrid Cloud

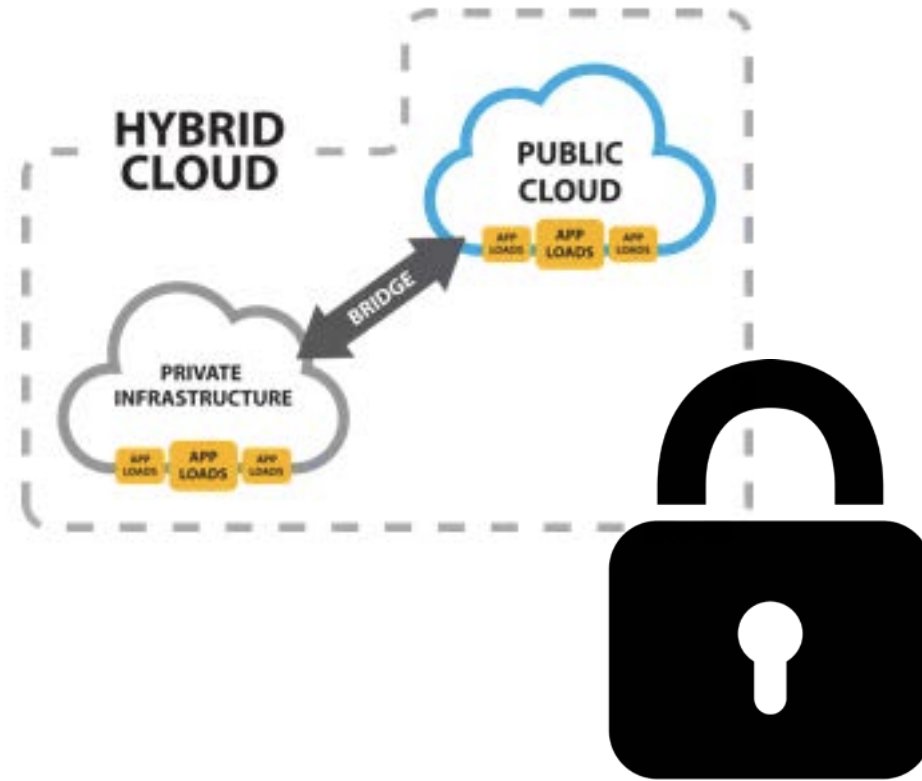


RackConnect

Services by popular public cloud service providers:

- AWS DirectConnect
- Azure Express Route
- Google CloudInterconnect
- ..

Securing a Hybrid Cloud



Security for On-Premise Enterprise Data Centre

Network Segmentation

- Network Segmentation based on trust models and application risk profiling



Host Security

- Hardened OS
- Host based Intrusion Detection/Prevention implemented
- Anti-virus/anti-malware protection



Application Security

- Secure coding practices
- Threat modelling
- Dynamic and Static Source code review
- Web Application Firewall
- API Gateway



Encryption

- SSL/TLS for data in transit
- Encryption at rest for sensitive information
- Key Generation and Management



Monitoring and Response via Security Operations Center

- Security Incident and Event Management solution
- Centralized security Log Management solution
- 24X7 Security Operations center



Network Protection

- Distributed Denial of Service Protection
- Firewalls to build visibility and mitigate any malicious activity
- Network Intrusion Detection/Prevention system to build visibility into any malicious network activity



Identity and Authentication

- Multi factor authentication
- Role based access management
- Periodic User ID Certification.



Server Security Assessments

- Vulnerability assessments via Nessus
- Minimum baseline security standards
- Penetration testing



Privileged User Access

- Privileged access to servers through multi-factor authentication
- Privileged user activity logging
- Remote Access to consultants/OEMs for support



Physical Security

- Building floor segmentation & access controls
- Visitor Management Systems
- Fire safety management, drills and audits
- Building Management System
- CCTV/PTZ cameras.
- Crisis Management Response and QRT

Security in Enterprise Data Centre | Private Cloud (2/2)



Security Governance

- Risk Management
 - Asset inventory and review
 - Incident Management
 - Security in change management
 - Crisis simulation and communication
 - Certifications against leading standards (ISO 27001:2013)
-



Policy and Processes

- Aligned with the global leading practices as outlined in the CSA, ISMS and ITIL frameworks
 - Governed through Information Security Policy
 - Compliance reporting to measure and continuously improve security posture
-



Privacy Controls

- Privacy program aligned with leading global privacy standards
 - Enabling privacy grievance officer by defining grievance redressal mechanism
 - Privacy impact assessments for enterprise and mobile applications
-

Security for hybrid cloud

Network Segmentation

- Network Segmentation Policy (Documented)
- VPC/VNET
- Dedicated connectivity with on-prem (expressroute/Dir onnect/Cloud Interconnect)



- Outbound Internet access through gateway

Host Security

- Host based Intrusion Prevention (HIPS)
- Anti-virus/anti-malware protection for Windows workloads



Application Security

- Secure coding practices
- Threat modelling
- Dynamic and Static Source code review
- Web Application Firewall
- API Gateway



Encryption

- SSL/TLS for critical data in transit
- SSL Offload for non-critical data
- Encryption at rest for sensitive information (S3/Blob)
- Key Management Services(Azure vault, AWS KMS)



Monitoring and Response via Security Operations Center

- CloudTrail/ELB/Azure LB Logs (integrate with on-premise Security Incident and Event Management)
- Log Management
- 24X7 Security Operations center



Network Protection

- DDoS Protection (Shield/CDN)
- Firewalls/Security Groups
- Network Intrusion Detection



Identity and Authentication

- Identity Federation
- Lockdown of Global Admin
- Enable Multi factor authentication
- RBAC for User IDs (incl. paid resources)
- User Roles with least privilege
- Roles for application



Server Security Assessments

- Vulnerability assessments and Patch Management
- Secure storage configuration (S3/Blob)
- Minimum baseline security standards (MBSS)
- Penetration testing



Privileged User Access

- Bastion Host/Enterprise PIM for privilege access to workloads
- Privileged user activity logging
- Rotate Keys regularly



Auditor's Perspective – What to Audit?

(1/3) Primary Control Procedures/ ITGC for a Financial Application

#	ITGC Category	Control Details	Technical Components	Additional Testing for Cloud?
1	Manage Change	Changes are Authorized, Tested, Approved and Monitored	Application, Interfaces, Database, OS and Network	Remain as-is. No change/additional testing required.
		Segregation of Duties	As Above	Check for IAM Roles to identify who all have right to make changes into the system.
2	Logical Access	General Systems Security as appropriate, Password Settings, Access to privilege IT functions and system resources, Logical Access is monitored, SoD	Application, Interfaces, Database, OS and Network Remote Access	Application Level – No Change. OS Level – <ul style="list-style-type: none">• Check for Identity Federation.• Check for MFA – Global and Regular.• Check for User Roles – Permissions to make changes to the workloads.• Permissions to make changes to the security groups. (Cont.)

Auditor's Perspective – What to Audit?

(1/3) Primary Control Procedures/ ITGC for a Financial

#	ITGC Category	Control Details	Technical Components	Additional Testing for Cloud?
3	Logical Access	New User setup process, Terminated/Transferred user Access.	Application, Interfaces, Database, OS and Network Remote Access	Application Level – No Change. OS Level – <ul style="list-style-type: none">• Check for access for the terminated/transferred users.• Changes made to the logical access are monitored.
4	Backup and Recovery	Data supporting financial application is backed-up and can be recovered.	Application, OS/Database	Instead of tapes, the auditor needs to test for Snapshots and cross-regional replication.
5	Scheduling, IT Incident Management	Scheduling of jobs (failures), and Incident Management	Application, OS/Database	Remain as-is.

Auditor's Perspective – What to Audit?

(2/3) ISO 27001 Information Security Management System

#	ISO 27001 Control Objective	Applicability (Cloud)	Technical Components	Remarks
1	A5 IS Policy	Yes	-	Applicable to On-Prem as well as Cloud.
2	A6 Organization of Information Security	Yes	-	Applicable to On-Prem as well as Cloud.
3	A7 Asset Management	Yes	Cloud Dashboard	Inventory and ownership of assets. Information Classification to remain as-is.
4	A8 Human Resource	-	-	Applicable to On-Prem as well as Cloud.
5	A9 Physical and Environmental Security	No	-	Not Applicable
6	A10 Communications and Operations Security	Yes	VPC/VNET, Security Groups, Expressroute/Direct Connect, Dashboard, Snapshot (for backup), S3/Blob Configuration, Internet Gateway.	Covers areas such as system planning, capacity planning & management, network security, backup and media handling. (Cont).

Auditor's Perspective – What to Audit?

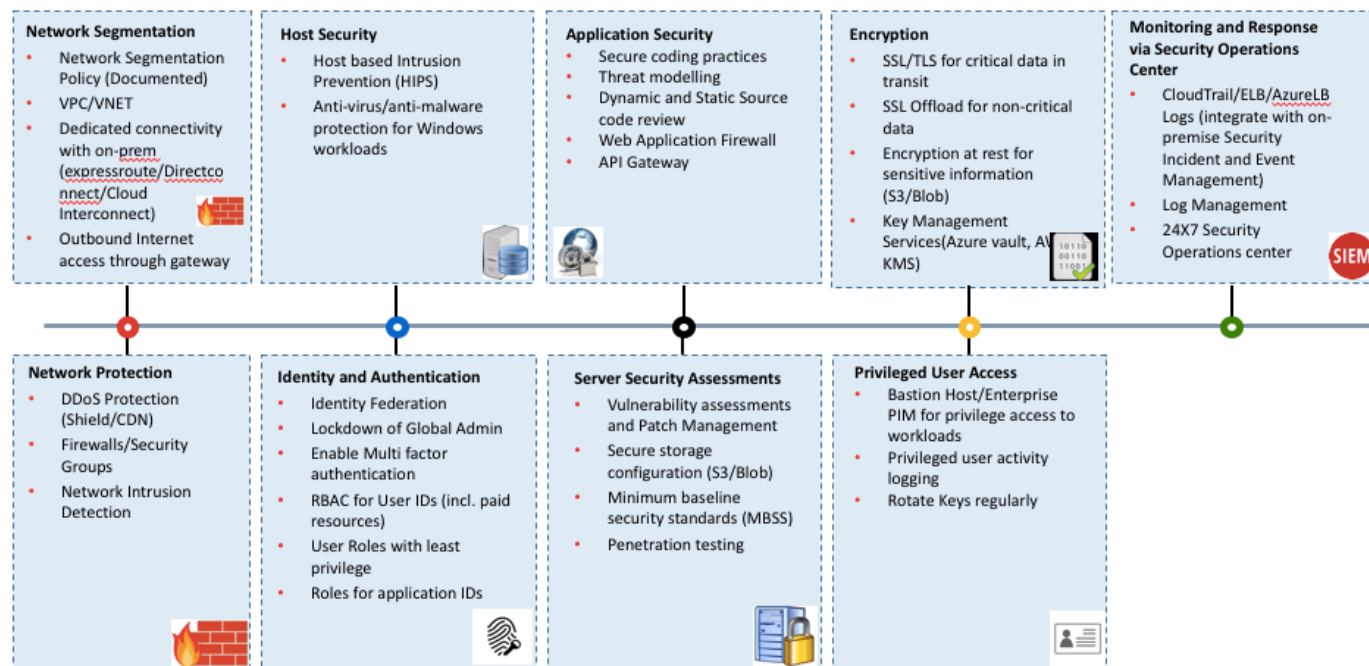
(2/3) ISO 27001 Information Security Management System

#	ISO 27001 Control Objective	Applicability (Cloud)	Technical Components	Remarks
6	A10 Communication and Operations Security	Yes	Log Management (API Logs/LB Logs)	Log Management and Monitoring.
7	A 11 Access Management	Yes	IAM, Identity Federation	User Identities and permissions.
8	A 12 Information System Acquisition, Development and Maintenance	Yes	VPC/VNET, Security Groups, KMS, Vulnerability Management and Patching.	Usage of production data in testing, and restricting Internet access. Cryptographic Controls.
9	A 13 Information Security Incident Management	Yes	SIEM and Incident Management Procedure.	
10	A 14 Business Continuity Management	Yes	Resilience using different availability zones/regions, recovery testing using snapshots	

Auditor's Perspective – What to Audit?

3/3) Cyber Security Review

- Not a checklist based audit.
- Understand the landscape.
- Perform threat modeling and create threat-vulnerability matrix.
- Identify Gaps in design and implementation.



Questions?

Thank you