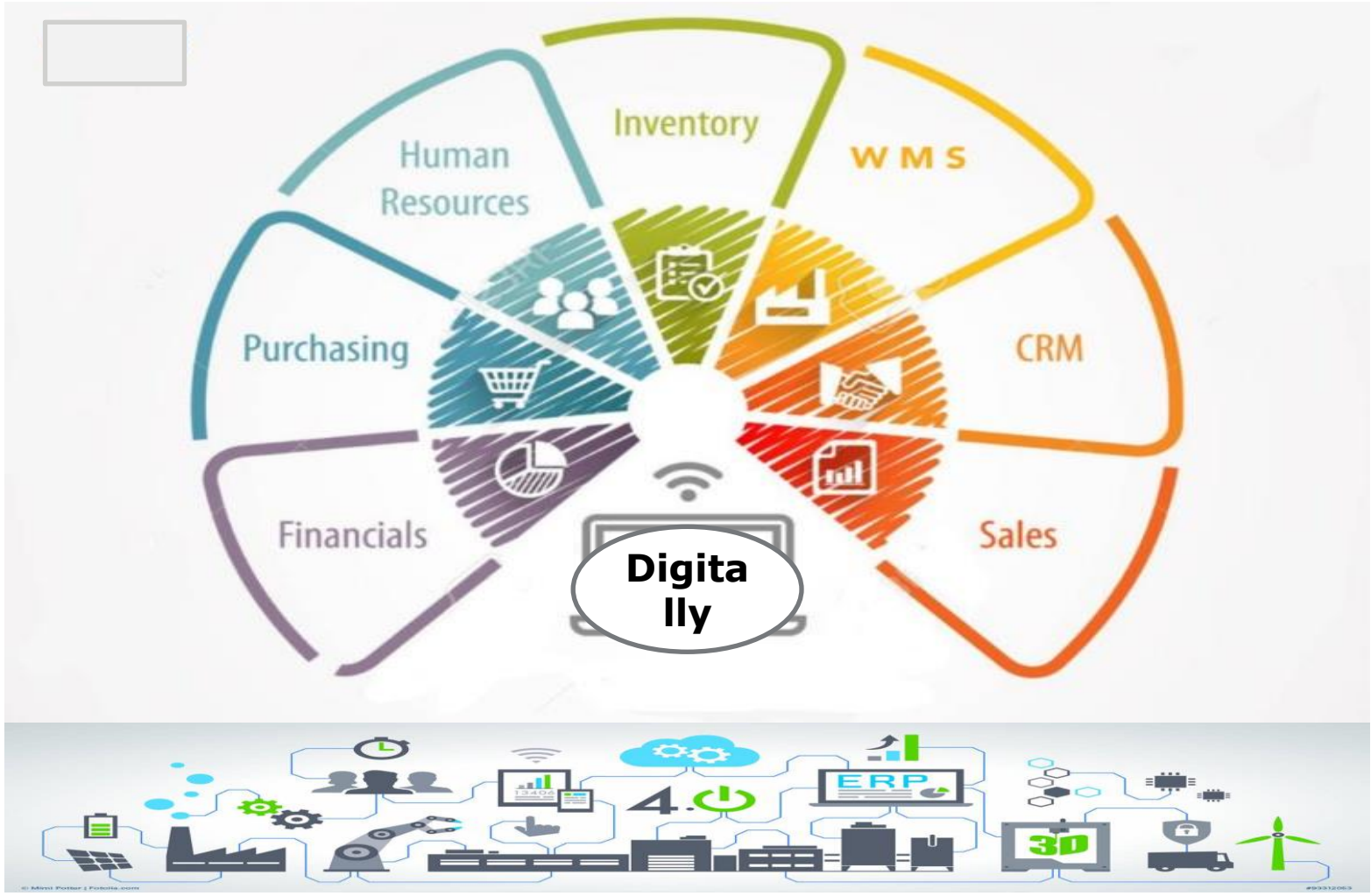
IT RISK MANAGEMENT AND CLOUD SECURITY

By CA Yukti Arora

Agenda

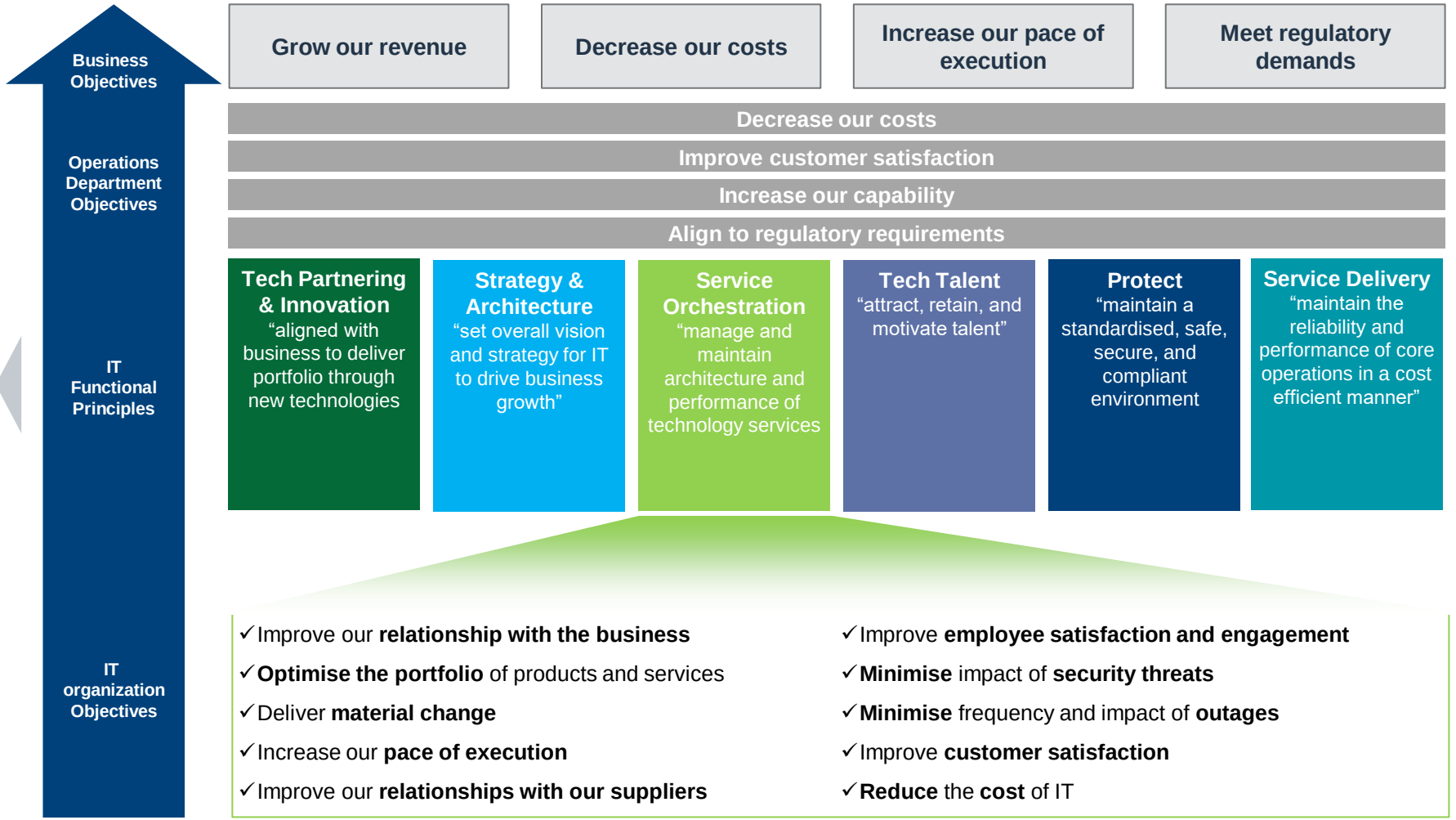
- Need for IT risk management
- Top 10 IT risk
- IT risk management framework
- Some IT risk and risk management strategies
- Cloud adoption in India
- Overview of cloud
- Cloud security risk and controls
- Some Cloud security logs
- Auditing cloud

HOW IS BUSINESS DONE NOWADAY



Technology deliver Business Strategy

THE IT ORGANIZATIONS EXIST TO PROVIDE SERVICES AND DRIVE VALUE FOR THE BUSINESS IN ACHIEVING ITS GOALS AND OBJECTIVES.



The objectives of the IT Organization directly feed into the wider objectives of the Business.

The IT Organization **performance management**

Top Risks

by likelihood

1. Extreme weather
2. Climate action failure
3. Human environmental damage
4. Infectious diseases
5. Biodiversity loss
6. Digital power concentration
7. Digital inequality
8. Interstate relations fracture
9. Cybersecurity failure
10. Livelihood crises

Top Risks

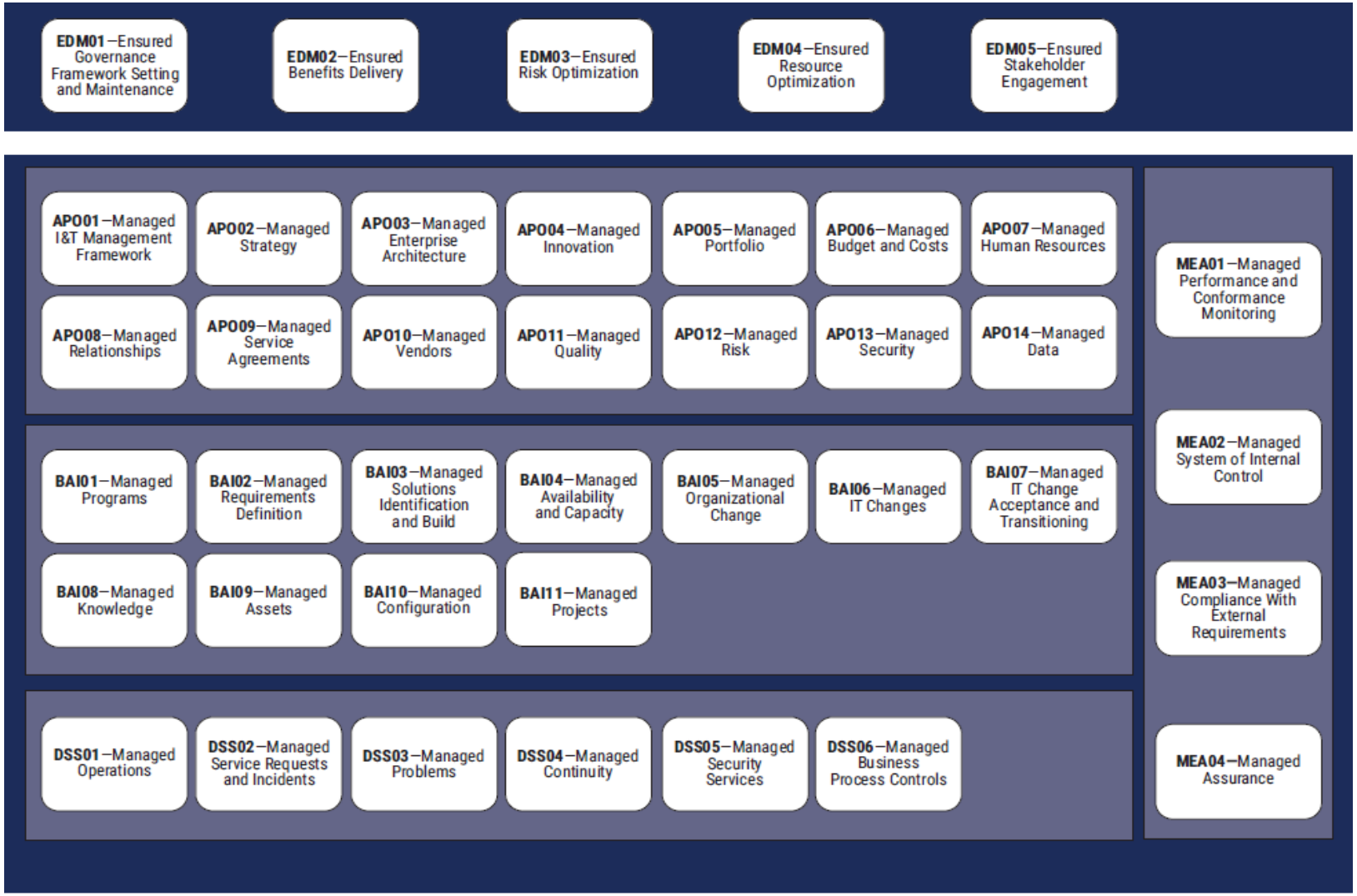
by impact

1. Infectious diseases
2. Climate action failure
3. Weapons of mass destruction
4. Biodiversity loss
5. Natural resource crises
6. Human environmental damage
7. Livelihood crises
8. Extreme weather
9. Debt crises
10. IT infrastructure breakdown

Source: https://www.weforum.org/agenda/2021/01/these-are-the-worlds-greatest-threats-2021/

IT Risk Management Framework

COBIT is an IT management framework developed by the ISACA to help businesses develop, organize and implement strategies around information management and governance.



Governance objectives are grouped in the **Evaluate, Direct and Monitor** (EDM) domain

Management objectives are grouped in four domains:

Align, Plan and Organize (APO) addresses the overall organization, strategy and supporting activities for I&T.

Build, Acquire and Implement (BAI) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.

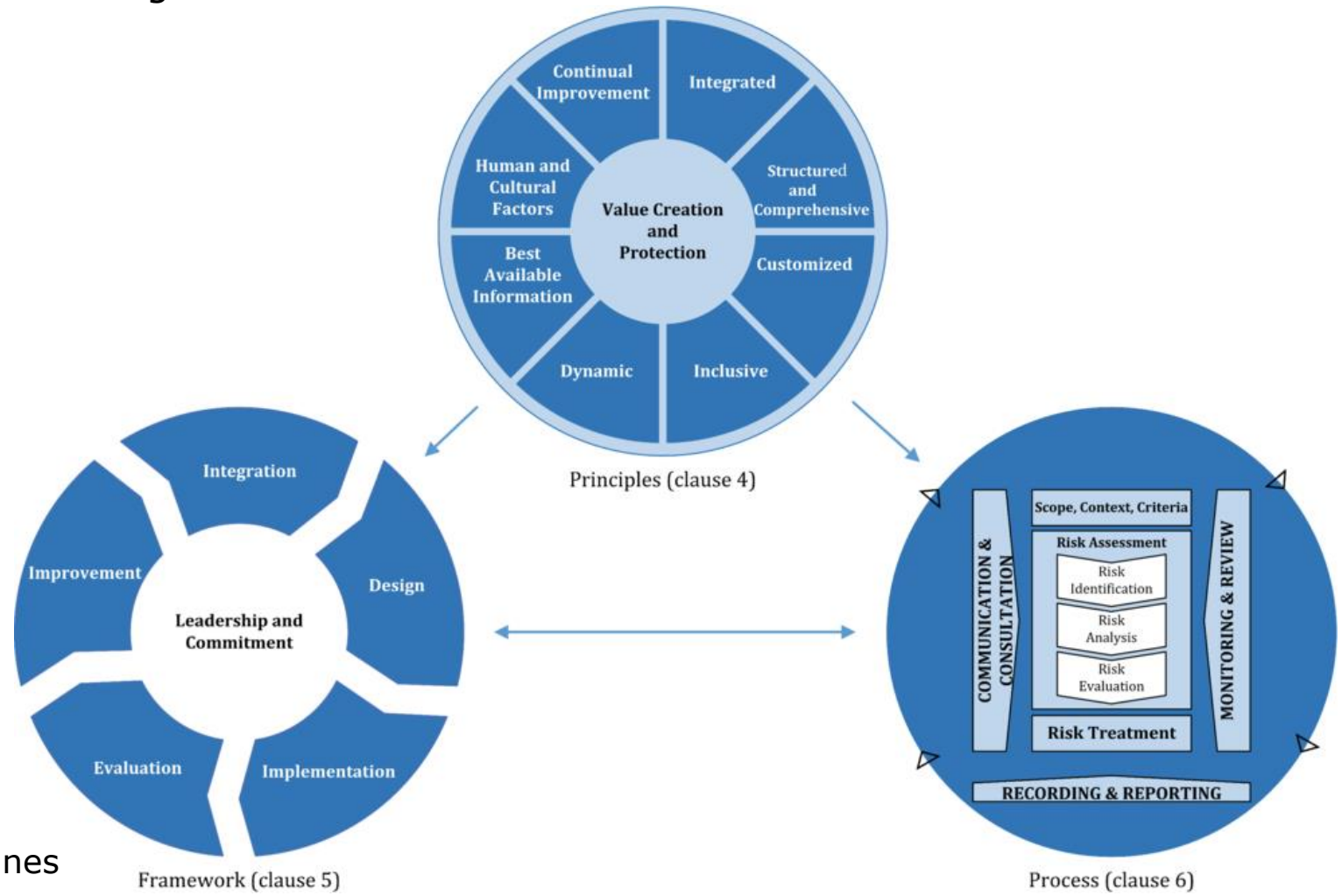
Deliver, Service and Support (DSS) addresses the operational delivery and support of I&T services, including security.

Monitor, Evaluate and Assess (MEA) addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements

Source:
COBIT 19- www.isaca.org

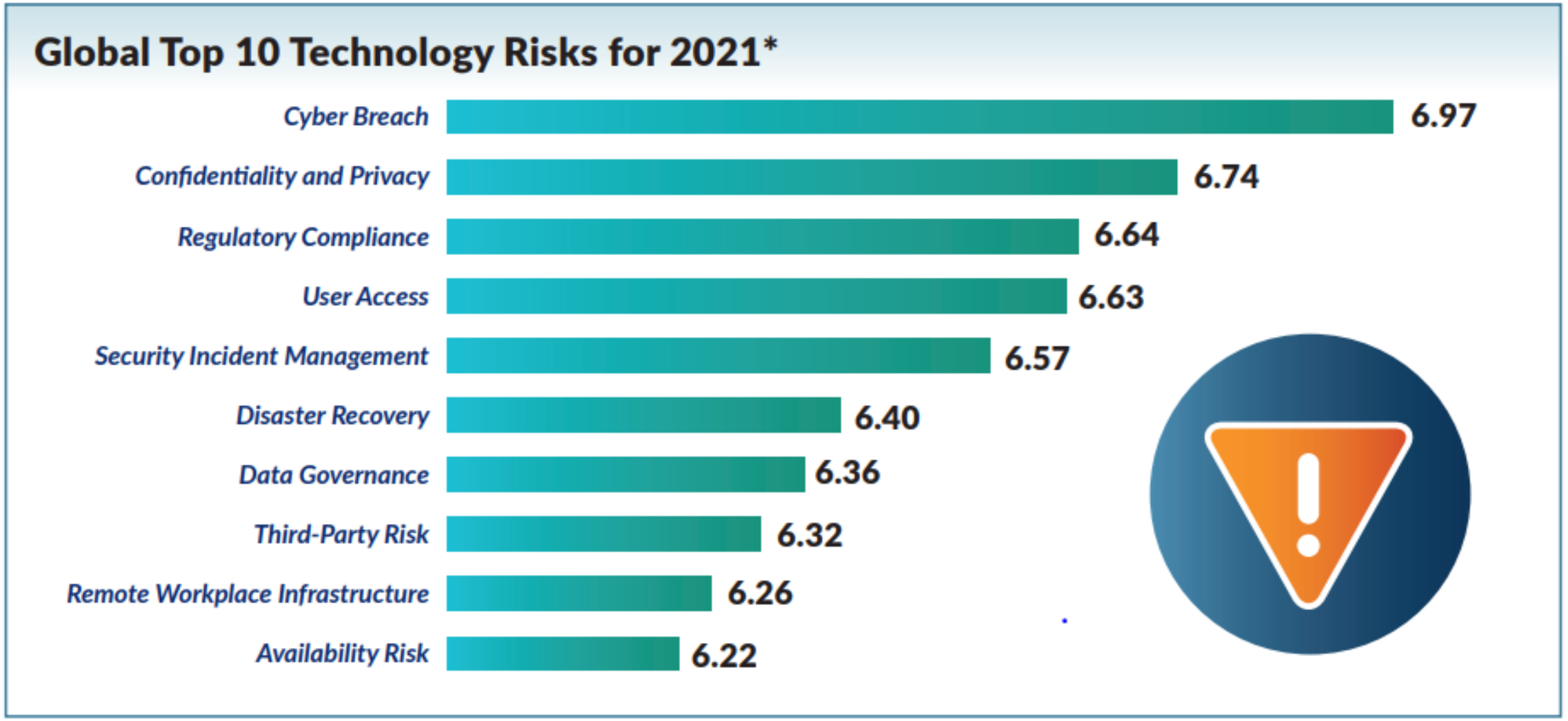
IT Risk Management Framework

ISO 31000 is an international standard that provides principles and guidelines for effective risk management. It outlines a generic approach to risk management for different types of risks and can be used by any type of organization. It provides guidelines and principles that can help to undertake a critical review of your organization's risk management.



Source:
ISO31000:2018 guidelines

Top Technology risk 2021 as per IT audit leaders



Source:
https://www.isaca.org

Summary of Top/ Principle Risks and risk management strategy

Sr. No.	Risk Area	Risk	Risk management strategy
1	Vulnerability & Cyber Risk Management	Risk of zero day threats, malware and other remerging threats and vulnerabilities.	1. Annual Comprehensive Internal and External CSA/VAPT Assessment of IT Landscape. 2. Implementation of Best in Class Security Tools. 3. IT Security Incident Monitoring and Advanced Threat Intelligence and Protection solution. 4. Continuous trainings & awareness programs. 5. Awareness mailers to be sent periodically.
2	BCP & DR	Risk of inadequate DR site for critical and significant applications and IT Infrastructure.	1. DR site for critical and significant applications and IT Infrastructure should be identified and tested (exercised) on an annual basis. 2. Plan for recovery of IT applications and corresponding infrastructure back to normal should be identified. 3. Review of Infrastructure and data availability for restoration testing. 4. DR Drills to be conducted and results must be documented. 5. Identification and documentation of single point of failure 6. Skill set and KPIs of BC Teams should be identified and reviewed annually.
3	Vendor/ Third Party Management	Risk of mismanagement of vendors which may result in lack of classification of vendors, their information, criticality of operations being handled by them.	1. Classification of vendor as per risk rating. 2. Third Party Risk assessment to be conducted for all vendors.
4	Cloud Security	Inadequate cloud strategy, due diligence of cloud from business objective , architecture alignment, may result in failure to obtain value from cloud adoption.	1. Clear cloud strategy and cloud road map should be prepared based on risk based assessment of cloud adoption. 2. Cloud Strategy should cover aspects of business objective, cloud architecture alignment, data governance, technology vendor landscape, Cyber and privacy security requirement. 3. Conduct security assessment or examine pre conducted security assessment report of vendor. 4. Legal vetting must be done from the perspective of jurisdiction, intellectual property laws and usage of shared resources. 5. Data protection impact assessment must be done. 6. SLAs should be monitored regularly for changing services, laws and regulations. 7. Train employees for operating in cloud environment.

Summary of Top/ Principle Risks and risk management strategy

Sr. No.	Risk Area	Risk	Risk management strategy
5	Human resource	Lack of succession planning and skill set on emerging tevhnology.	1. Continuous upskilling trainings & awareness programs. 2. Succession planning to develop IT leadership.
6	Regulatory Compliance	Increase cross border Cyber, privacy and IT compliance	1. IT Compliance framework Design, implementation and monitoring . 2. Building system which have security, privacy, controls including audit logging and monitoring by design
7	Mobile Device & Teleworking –Work from Home	Work from home related security risk, wherein due to failure of defense against attackers on endpoints or mobile device there could be threats like multi stage attacks, fileless malware, and malicious insiders.	1. User should login through VPN while logging through home networks/public networks. 2. VPN access should be provided based on approval by authorized person. 3. Endpoint solution should be implemented after conducting due diligence regarding security and privacy, POC w.r.t. to business object achievement and alignment with value delivery and budget allocation. 4. Incident Management and response team must be identified.
8	Data Governance, confidentiality and privacy	Risk of DLP not being proactive by preventive automated controls, detective controls may delay the response on loss of data.	1. DLP tool should be configured for preventive, analysis and blocking on proactive basis. 2. DLP incident monitoring.
9	IT infrastructure availability	Risk of IT infrastructure breakdown leading to IT not being able to support business objective.	1. Component level redundancy w.r.t. IT infrastructure is established to support business in case of hardware/ software failure. 2. SLAs including escalation matrix with vendors providing critical infrastructure support and maintenance has been defined. 3. Review of AD, network and hardware availability for restoration testing is conducted on a timely basis.
10	Strategy	Risk of IT operation in silo leading to lack of knowledge management, synergy, collaboration resulting in lack of achievement of IT objectives.	1. KPI's knowledge sharing at function level to be defined. 2. Periodic steering committee meeting to be planned with relevant stakeholders for group brainstorming and comprehensive assessment of risk and adequate measures for the same. 3. Collaborative interaction and Skill set diversity

Cloud adoption current scenario in India as per NASSCOM

1. India's Public Cloud market stands at ₹ 170 billion in FY2020 and is growing at ~30% CAGR till FY2025 to reach ₹ 630 billion

2. In a survey of 1000+ SMBs in India, 60% are already using cloud, though almost half are at early stages of adoption

3. Best in class SMBs that adopted cloud have been able to drive 25-30% productivity improvement and 15-20% reduction in operational costs.

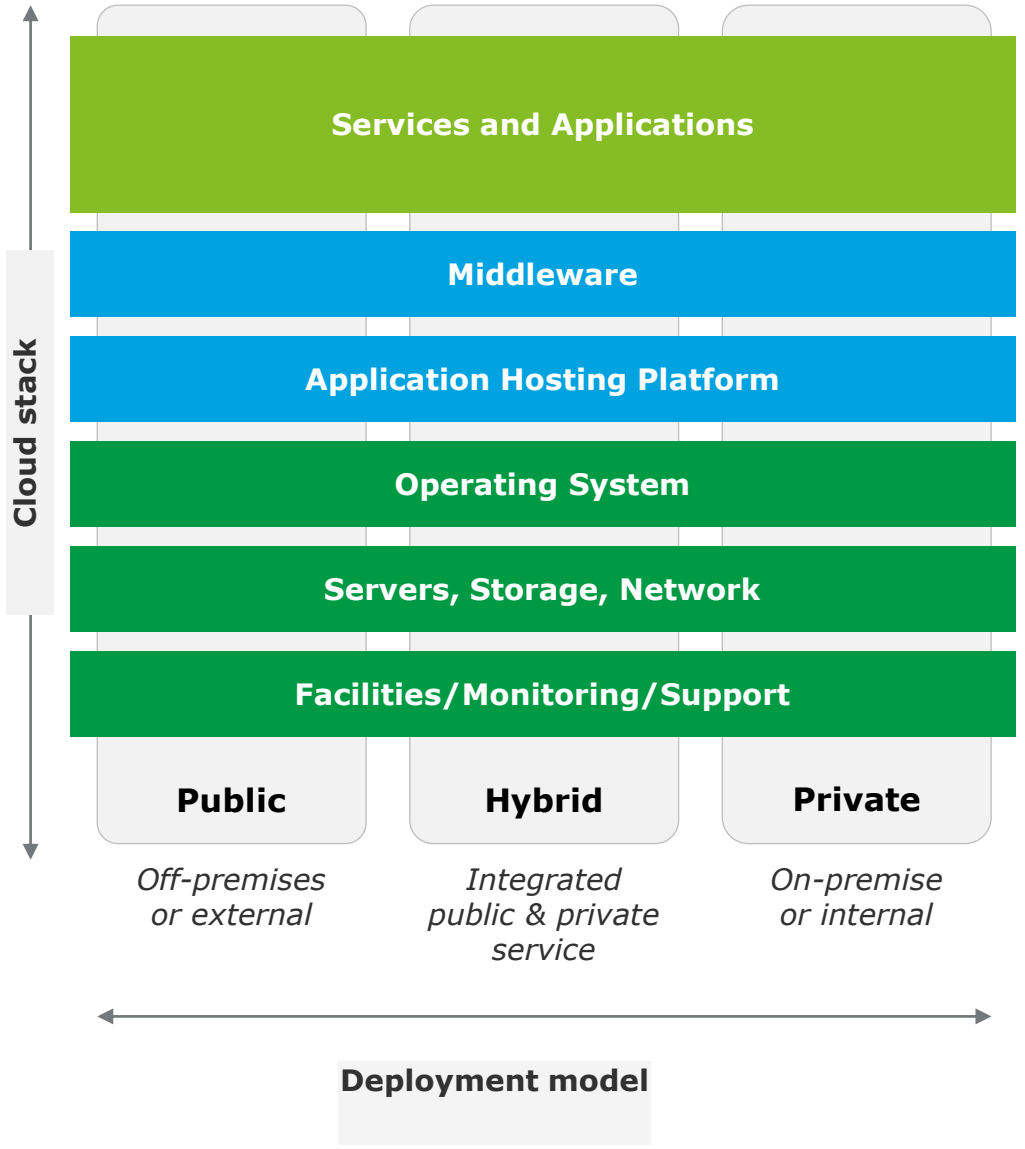
4. Security, Analytics and Offline to Online are the three major opportunity segments for cloud adoption

5. More than 50% of respondents cite lack of management support, talent and capital as key constraints for cloud adoption

6. Progressive policies and awareness programs can accelerate cloud adoption

NASSCOM®

OVERVIEW OF CLOUD COMPUTING



Software-as-a-Service

Software that provides a specific built-for-purpose business service to the client

Platform-as-a-Service

Ready-to-use scalable integrated application and data hosting

Infrastructure-as-a-Service

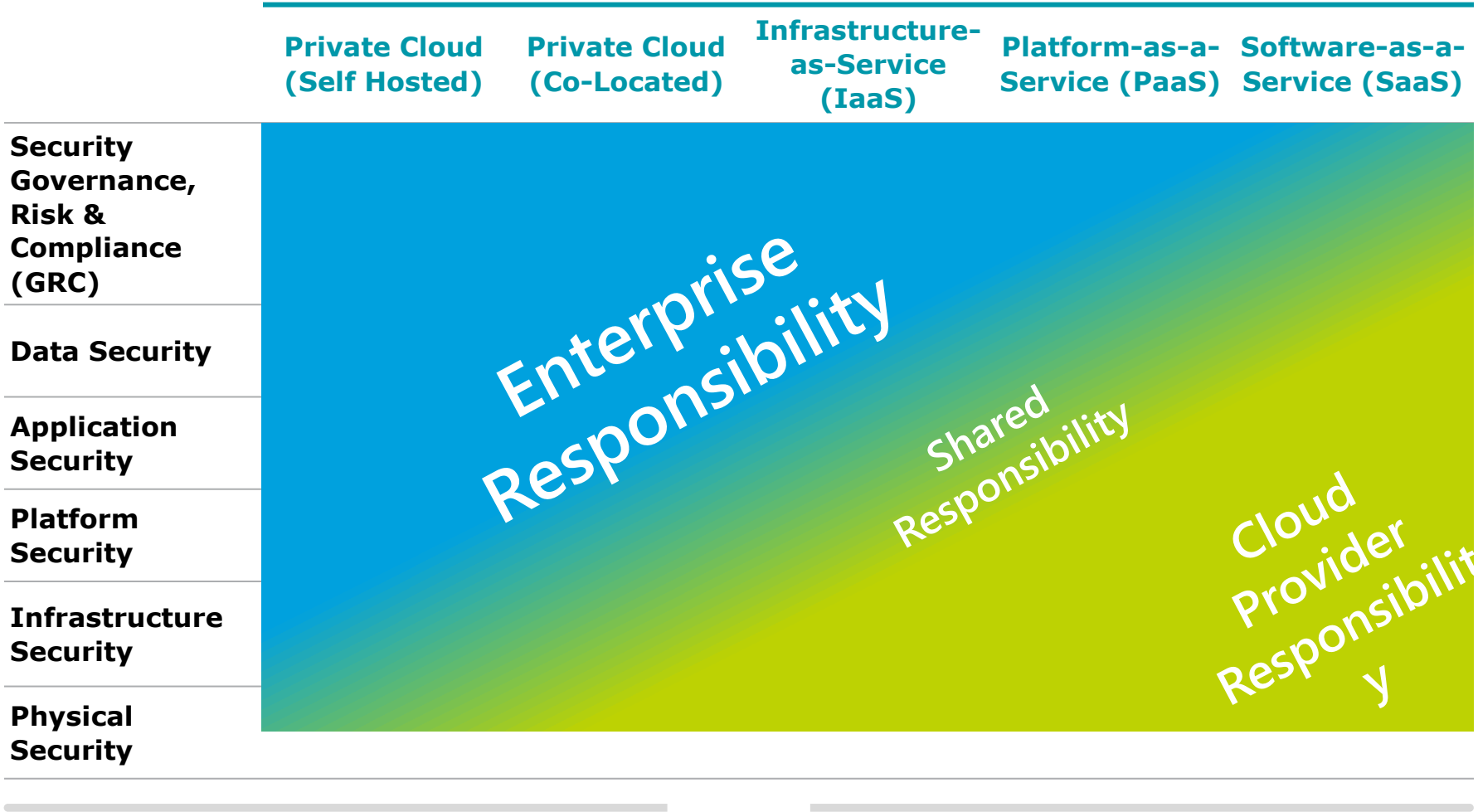
Horizontally scalable compute, storage and networking delivered to an application on-demand

NIST DEFINITION OF CLOUD COMPUTING INDICATES THAT THE CLOUD IS COMPOSED OF FIVE ESSENTIAL CHARACTERISTICS:

Broad Band Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms
On-demand Self Service	Cloud computing is highly available and scalable: Replication is part of the cloud framework. Use as needed, resources can be turned on or off quickly and as needed including storage capacity, databases, web servers and operating systems without human intervention
Resource Pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
Rapid Elasticity	Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).

CLOUD SERVICE MODELS – SERVICE DELIVERY ACROSS IT LAYERS

Responsibility Chart



CYBER RISKS IN CLOUD COMPUTING

There are a variety of cyber risks associated with moving to the cloud, yet there is also an opportunity

Concentrated Risk
Cloud providers are a bigger target because "that's where the data is"

Consumer/Shadow IT
Business and consumers using cloud with or without cyber controls

Third-party Risk
Enterprises are dependent on cloud providers' controls

Modern Attack Surface
The walled enterprise is replaced by a hybrid, more complicated technology environment

Controls Gap
Traditional cyber risk controls need to extend to the cloud at a time when many enterprises are barely keeping up with existing threats

Cyber Risks In Cloud Computing

Protecting cloud infrastructure needs security re-architecture

Data Protection	• Revisit data asset inventory, classification, and implement tagging • On premise or in the cloud data protection tools? • Data residency, privacy, and compliance based on cloud use cases
Virtualized Network & Infrastructure	• Configuring cloud provider proprietary IaaS and PaaS services appropriately • Securing ingress/egress between traditional enterprise and other cloud providers • Segmentation, micro-segmentation for hybrid cloud (subnets, firewalls, NACLs (Network Access Control List), etc.) • Integrating policy enforcement in IaaS, PaaS, and virtual network as software • Harden virtual servers and endpoints
DevSecOps	• Adapt a culture of DevSecOps with guardrails and compliance validations • Integrate security controls into system development lifecycle (automated CI/CD (Continuous Integration and Deployment) • Extend protection and scanning of new infrastructure and automation source code components
Vigilant	• Achieving comprehensive visibility for cloud down to the guest-level • Keeping up with elastic environments with proprietary IaaS and PaaS technology • Use on-premise SIEM or build new one in the cloud?
Resilient	• Designing resilient cloud architectures • Refreshing data backup and archiving for IaaS and PaaS • Ensuring incident management and response capabilities are updated for cloud

SOME GOVERNANCE CONTROL CONSIDERATION

Governance vs. Lack of Governance

What issues have you experienced?

SOME CLOUD— IT CONTROL

Common IT Control

Information Security	
Logical Access Controls	Data Encryption
Network Configuration Management	Security Monitoring and Logging

Change Management	
IT Asset Identification	Asset Configuration and Management

IT Operations	
IT Asset Configuration	Security Monitoring and Logging
Data Encryption	Disaster Recovery
Security Incident Response	

Billing and Monitoring
Financial Controls

CLOUD— FEW OTHER CONTROL AREA CONSIDERATIONS (CONT.)

Use Case: Significance of Logging Telemetry

List of different Cloud logs showing description and benefits of logging.

Log Sources	Description of Logged Data	Benefits of Logging
CloudTrail	With CloudTrail, you can log, continuously monitor, and retain events related to **API calls** across your Cloud infrastructure.	• Analyze access attempts via API calls • Track changes to Cloud resources
Virtual Private Cloud (VPC) Flow Logs	VPC flow logs is a feature that enables you to capture information about the **IP traffic** going to and from network interfaces in your VPC.	• Identify bottlenecks in network processing • Identify and analyze root cause of malicious traffic
Cloud Config	Cloud Config is a service that enables you to assess, audit, and evaluate the configurations of your Cloud resources.	• Identification of resource configurations that deviate from your organization's policies and guidelines • Ability to create and maintain a dashboard of historical configuration changes
Elastic Load Balancer (ELB) Access Logs	Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer.	• Detect/prevent malicious activities • Identify and troubleshoot issues that might be affecting the end users
Web Access Firewall (WAF) Logs	The log details for WAF restricted traffic flows via ELB logs or CloudFront logs.	• Detect/prevent malicious activities • Identify and troubleshoot issues that might be affecting the end users

CLOUD— FEW OTHER CONTROL AREA CONSIDERATIONS (CONT.)

Use Case: Significance of Logging Telemetry

List of different Cloud logs showing description and benefits of logging.

Log Sources	Description of Logged Data	Benefits of Logging
Inspector Assessment Reports	• An assessment report is a document that details what is tested in the assessment run and the results of the assessment.	• Prioritized and timely fix of vulnerabilities • Tracking compliance to the policy of recurring vulnerability assessments
S3 Logs	• S3 logging provides a way to get detailed access logs which contain details about the request, such as the request type, the resources specified in the request worked, and the time and date the request was processed.	• Understand customer behaviors so that organization can design the architecture to make popular objects more accessible • Logging increase visibility of each request made to your bucket and corrective controls can be implemented based on logging data
Relational Database Service (RDS) Logs	• This is used for logging the database log file including the general and error log file for RDS instances.	• Monitoring disk space consumption • Monitoring database network traffic
Lambda Logs	• We can insert logging statements into our Lambda code to help us validate that our code is working as expected.	• To determine cause of increased latency in the execution of a Lambda function

CLOUD SERVICE MODELS – CONTROLS TESTED AT DIFFERENT LAYERS

Below is a typical chart of the level of ability to audit and responsibilities around assurance changes, but this could vary depending on the contract and Cloud Services Provider solution. (CSP)

	In House	IaaS CSP	PaaS	SaaS
Physical	Audit Directly	Rely on Third Party/SOC2/Contract consider UCC	Rely on Third Party/SOC2/Contract consider UCC	Rely on Third Party/SOC2/Contract consider UCC
Management Console	Audit Directly	Rely on Third Party/SOC2/Contract consider UCC	Rely on Third Party/SOC2/Contract consider UCC	Rely on Third Party/SOC2/Contract consider UCC
Hyper Visor/Data Storage/File Storage	Audit Directly	Rely on Third Party/SOC2/Contract consider UCC	Rely on Third Party/SOC2/Contract consider UCC	Rely on Third Party/SOC2/Contract consider UCC
Servers and Operating Systems	Audit Directly	Audit Directly	Rely on Third Party/SOC2/Contract consider UCC	Rely on Third Party/SOC2/Contract consider UCC
Middleware/Software Stack	Audit Directly	Audit Directly	DirectlyAudit/ Rely on Third Party/SOC2/Contract consider UCC	Rely on Third Party/SOC2/Contract consider UCC
Application	Audit Directly	Audit Directly	Audit Directly	Audit Directly

Thank you.