# Legal, Risk, and Compliance Slide Deck for Cloud Computing

## CCSP Series - Chapter # 6b

# Cloud Computing & Enterprise Risk Management Evolution

- **Overview of IT Landscape Shifts**

> - **Two decades ago:** System provisioning took days or weeks.
> - **Dot-com era vs. Today:** From months to minutes for system setup.

- **Impact on Enterprise Risk Management**

> - Accidental server provisioning was unlikely historically.
> - **Current cloud scenarios:** Rapid infrastructure setup, including international locations.
> - Emergence of new risks and management strategies.

# Cloud Risk Management Strategy Evolution

## 1 Changing Risks & Strategies

- Understand changes in enterprise risk management.
- Adaptation to cloud computing's fast-paced evolution.

## 2 Need for Updated Risk Approaches

- Novel strategies employed for risk mitigation.
- New assessment, evaluation, and communication methods.

# Assessing Cloud Provider's Risk Management Programs

### Before Partnership: Risk Analysis

- Analyze risk associated with cloud provider's services.
- Reliance on Supply Chain Risk Management (SCRM) due to shift in IT control.

### Evaluating Supplier Risk Programs

- Check for risk management program existence.
- Adequacy issues addressed via indirect audits like SOC 2, ISO 27001.

# Audits and Compliance – Indirect Assurance

- **Frameworks for Audit Reports**

> - SOC 2, ISO 27001, FedRAMP, CSA STAR.
> - Third-party auditors and framework-based reports.

- **Selecting Compliant CSPs**

> - Compliance with specific frameworks (e.g., FedRAMP for U.S. government).
> - Considerations of audit scope and relevance to services used.

# Understanding Risk Profiles & Appetite

## 1 Risk Profile Considerations

- Determined by identified risks and mitigations.
- **Tech startups vs. Financial firms:** Risk and regulation vary.

## 2 Defining Risk Appetite

- Organizations' willingness to accept risk.
- **Startups vs. Established Companies:** Risk acceptance based on available resources.

# Data Ownership & Processing in Cloud

### Categories of Data Responsibility

- **Data Subject:** Individual/Entity whose data is processed.
- **Data Controller:** Decides how and why data is processed, owns risk.
- **Data Processor:** Processes data on behalf of the controller, implements protections.

### Legal and Regulatory Implications

- **Data breaches:** Liability often sits with data controller.
- **Data processors:** Custody responsibilities specified via contractual clauses.

# Regulatory Frameworks and Transparency in Cloud

- **Breach Notification Rules**

> - Regulations (GDPR, HIPAA, etc.) require timely notifications post-breach.

- **Sarbanes-Oxley Act and GDPR Overview**

> - **SOX:** U.S. Act for publicly traded companies ensuring transparency.
> - **GDPR:** EU regulation demanding clear communications about data processing.

# Effective Risk Treatment Techniques

## 1 Identifying and Assessing Risks

- **Risk assessment:** Measuring likelihood and impact.
- Priority given to risks with greater impact and likelihood.

## 2 Risk Treatment Options

- Avoidance, Transfer (e.g. Insurance), Mitigation, Acceptance.
- Balancing cost-benefit in adopting controls.

# Risk Management Frameworks to Consider

**ISO 31000:2018 - Risk Management Guidelines**

- **Strategies to lower risk:** Avoidance, Acceptance, Sharing, Retention.

**Cloud-Specific Risk Management**

- ENISA's risk assessment tool for cloud.
- NIST SP 800-146 and 800-37 for lifecycle risk management approach.

# Cybersecurity Metrics and Key Risk Indicators

- **Tracking Risk Management Efficacy**

> - Patching levels and deployment timeframes.
> - Intrusion attempts and their frequency.
> - Mean Time To Detect, Contain, and Resolve Incidents.

# Assessing Cloud Risk Environment

### Key Questions When Choosing a CSP

1. Provider's stability, legal jurisdictions, and outstanding legal issues.
2. Service pricing protections and compliances.
3. Backup, recovery, and failover processes.

# Information Security Buzz

Discover more at our InfoSec Knowledge Hub