

# WEEK 11: MANAGING CLOUD RISKS



# WORKFORCE DEVELOPMENT



# Content Usage Parameters

**Content** refers to material including instructor guides, student guides, lab guides, lab or hands-on activities, computer programs, etc. designed for use in a training program



1

Content is subject to  
copyright protection

2

Content may only be  
leveraged by students  
enrolled in the training  
program

3

Students agree not to  
reproduce, make  
derivative works of,  
distribute, publicly perform  
and publicly display in any  
form or medium outside of  
the training program

4

Content is intended as  
reference material only to  
supplement the instructor-  
led training

# REVIEW: WEEK 10

## Overestimating Cost Savings:

Understand hidden migration fees, underestimated operational expenses, and the complexities of Azure's consumption-based pricing.

## Data Transfer & Integration Issues:

Recognize challenges with legacy system integration, unexpected data egress fees, and performance impacts.

## Security & Compliance Gaps:

Identify risks from misconfigurations, inadequate access controls, and the importance of continuous monitoring using tools like Azure Security Center.

## Skills and Training Deficiencies:

Highlight the need for ongoing education, certification programs, and knowledge sharing to bridge the cloud skills gap.

## Vendor Lock-In & Performance Monitoring Challenges:

Emphasize the risks of over-dependence on a single vendor and the necessity of unified dashboards for real-time performance tracking.

- Week 1-2: Introduction to Cloud Technology
- Week 3-5: Cloud Strategy and Architecture
- Week 6-7: Use Cases and Real-World Applications
- Week 8-9: Benefits and Value Proposition
- Week 10-12: Challenges and Risks
- Week 13-14: Interactive Simulations and Practical Exercises
- Week 15: Course Review and Final Assessment

# OVERVIEW

**Risk Identification:** Recognize potential vulnerabilities

**Governance Frameworks:** Establish robust policies

**Security Best Practices:** Protect data and applications

**Vendor Management:** Mitigate dependency risks

**Continuous Monitoring:** Ensure ongoing risk assessment

# CLOUD RISK IDENTIFICATION

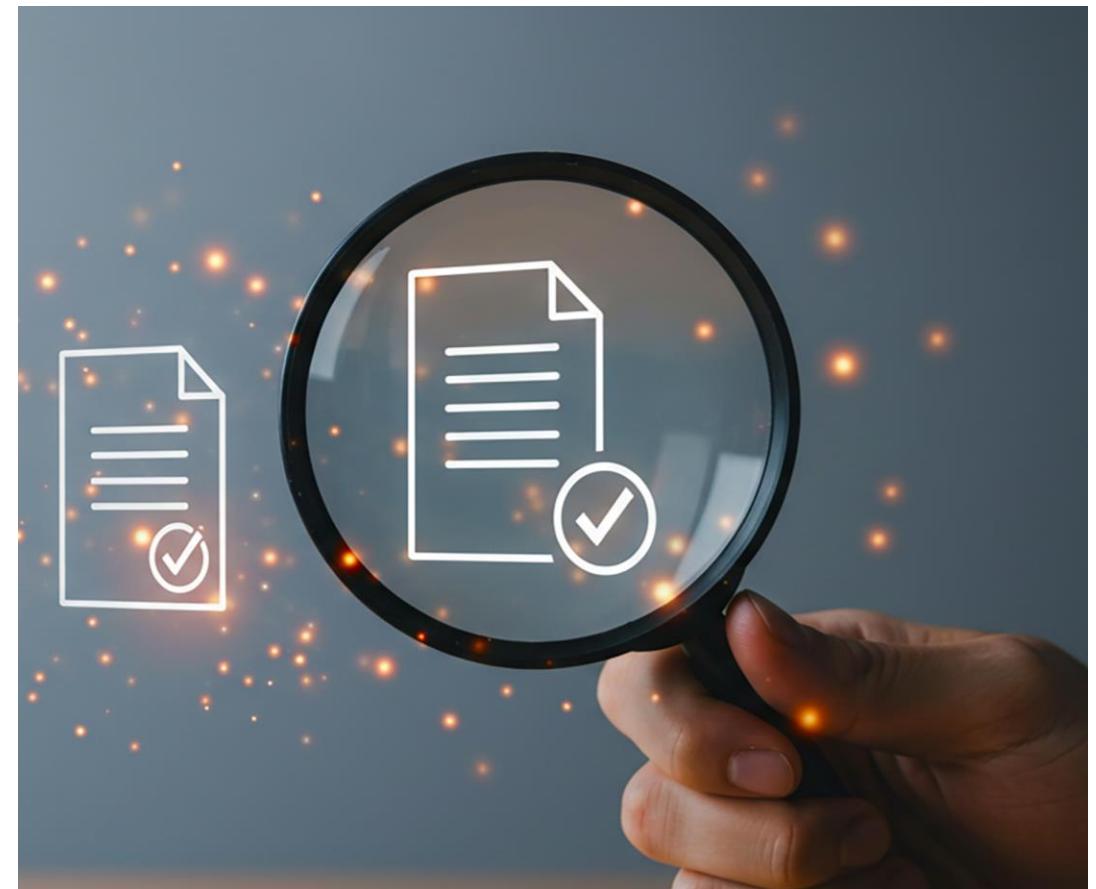
**Definition:** Identifying potential vulnerabilities in cloud environments

**Importance:** Proactive risk management to prevent breaches and ensure compliance

**Overview:** Process involves assessing threats, vulnerabilities, and impacts

**Key stakeholders:** IT, security teams, executive leadership

**Tools and frameworks:** Essential for systematic identification e.g. NIST Cybersecurity Framework



# CASE STUDY



The 2019 Capital One breach, where a misconfigured AWS firewall exposed data of over 100 million customers, underscores the need for robust risk identification.

Regular audits could have prevented this incident (CSO Online).

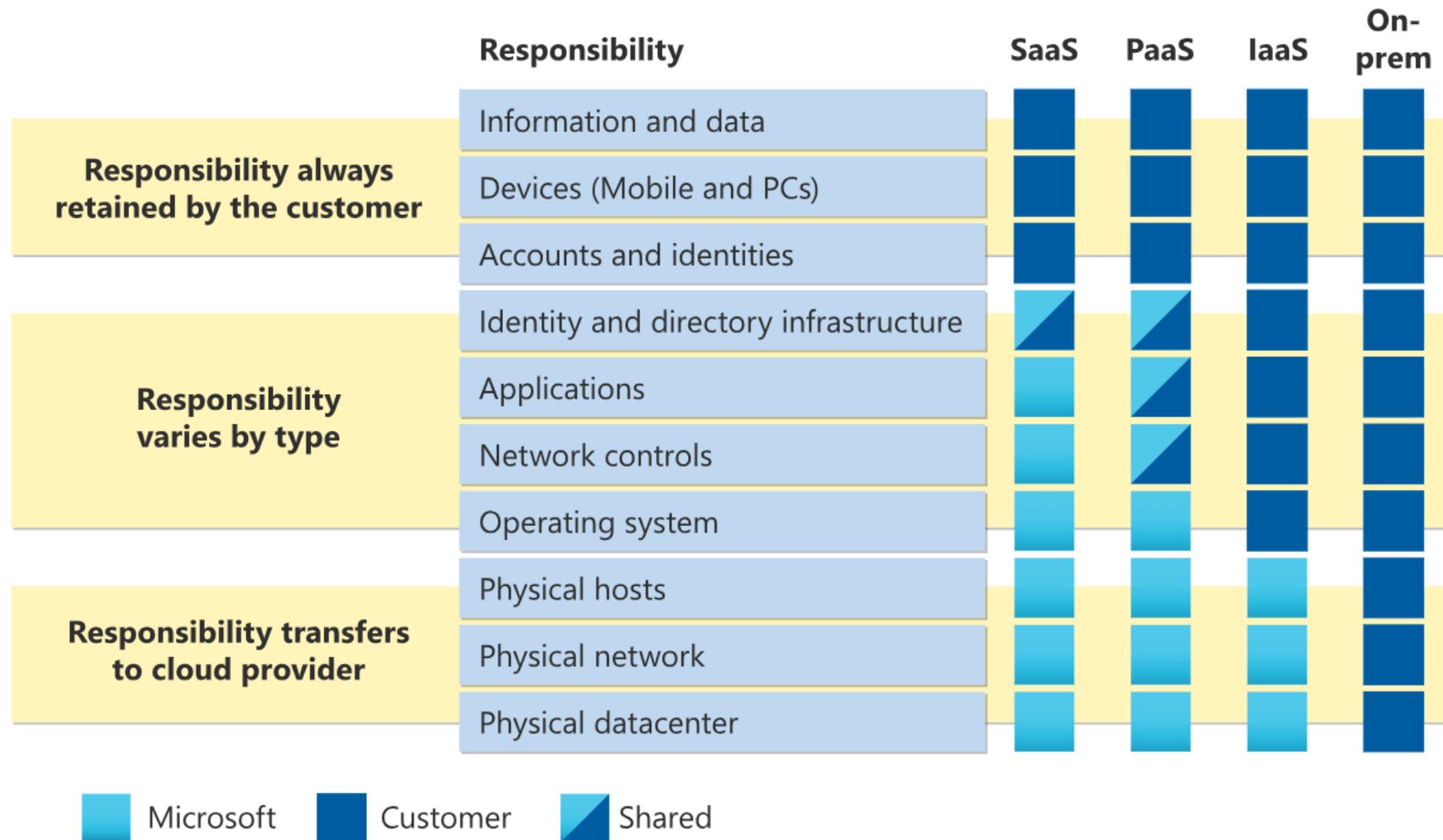
# TYPES OF CLOUD RISKS



# RISK IDENTIFICATION METHODS

- Threat modeling: Mapping potential attack vectors
- Vulnerability scanning: Automated detection of weaknesses
- Penetration testing: Simulating real-world attacks
- Compliance audits: Ensuring regulatory adherence
- Regular security assessments: Ongoing risk evaluation

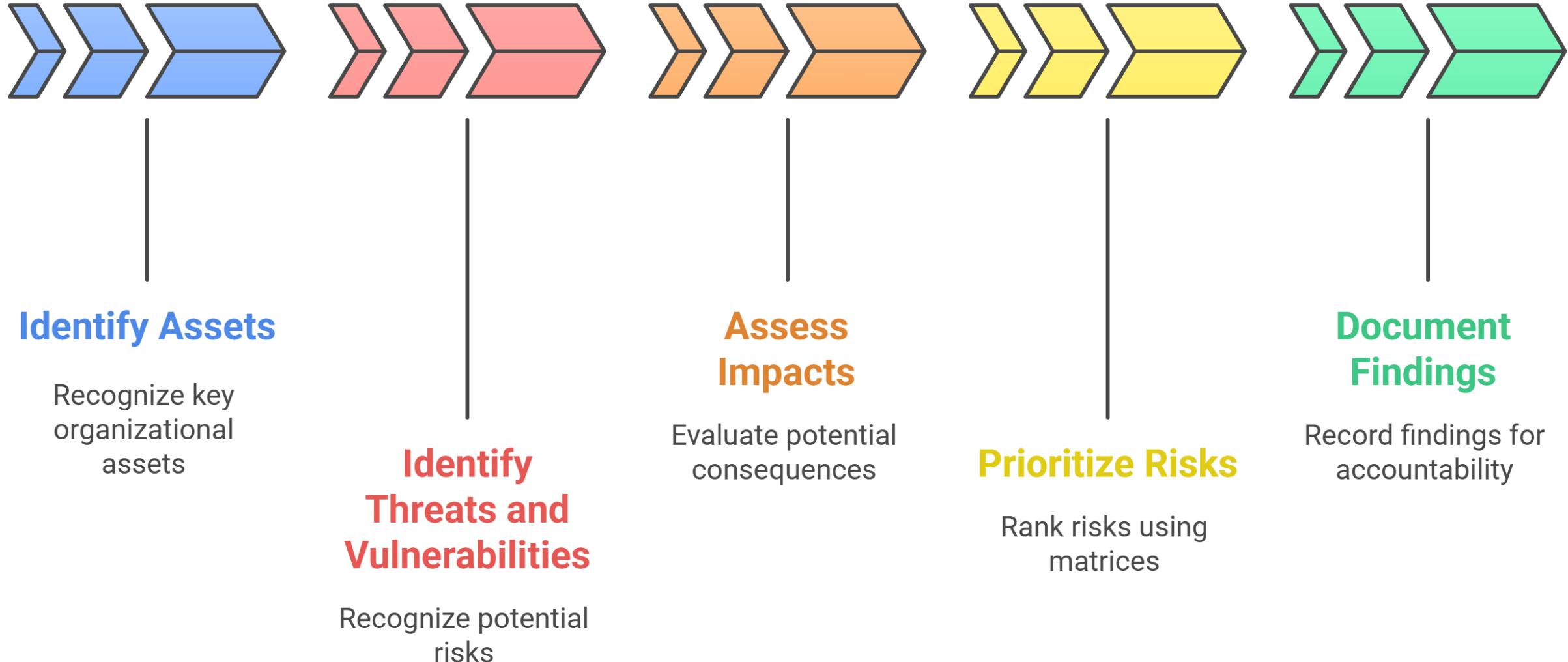
# SHARED RESPONSIBILITY MODEL



# RISK ASSESSMENT FRAMEWORKS

- NIST Cybersecurity Framework: Structured risk management
- ISO/IEC 27001: Information security standard
- CSA Cloud Controls Matrix: Cloud-specific controls
- CIS Controls: Prioritized security recommendations
- Selection based on industry, compliance needs

# CONDUCTING A RISK ASSESSMENT



# TOOLS FOR RISK IDENTIFICATION

- CSPM tools: Lacework, Prisma Cloud
- Vulnerability management: Qualys, Tenable
- Threat intelligence platforms
- Compliance management tools
- SIEM integration for visibility

# GOVERNANCE & COMPLIANCE



**Policy Development:** Create clear governance policies

**Regulatory Alignment:** Comply with industry standards

**Risk Assessments:** Conduct regular audits

**Role Definition:** Clearly assign responsibilities

**Azure Tools:** Utilize Azure Policy and Blueprints

# STRATEGIES FOR GOVERNANCE

**Develop Frameworks:** Establish organizational governance models

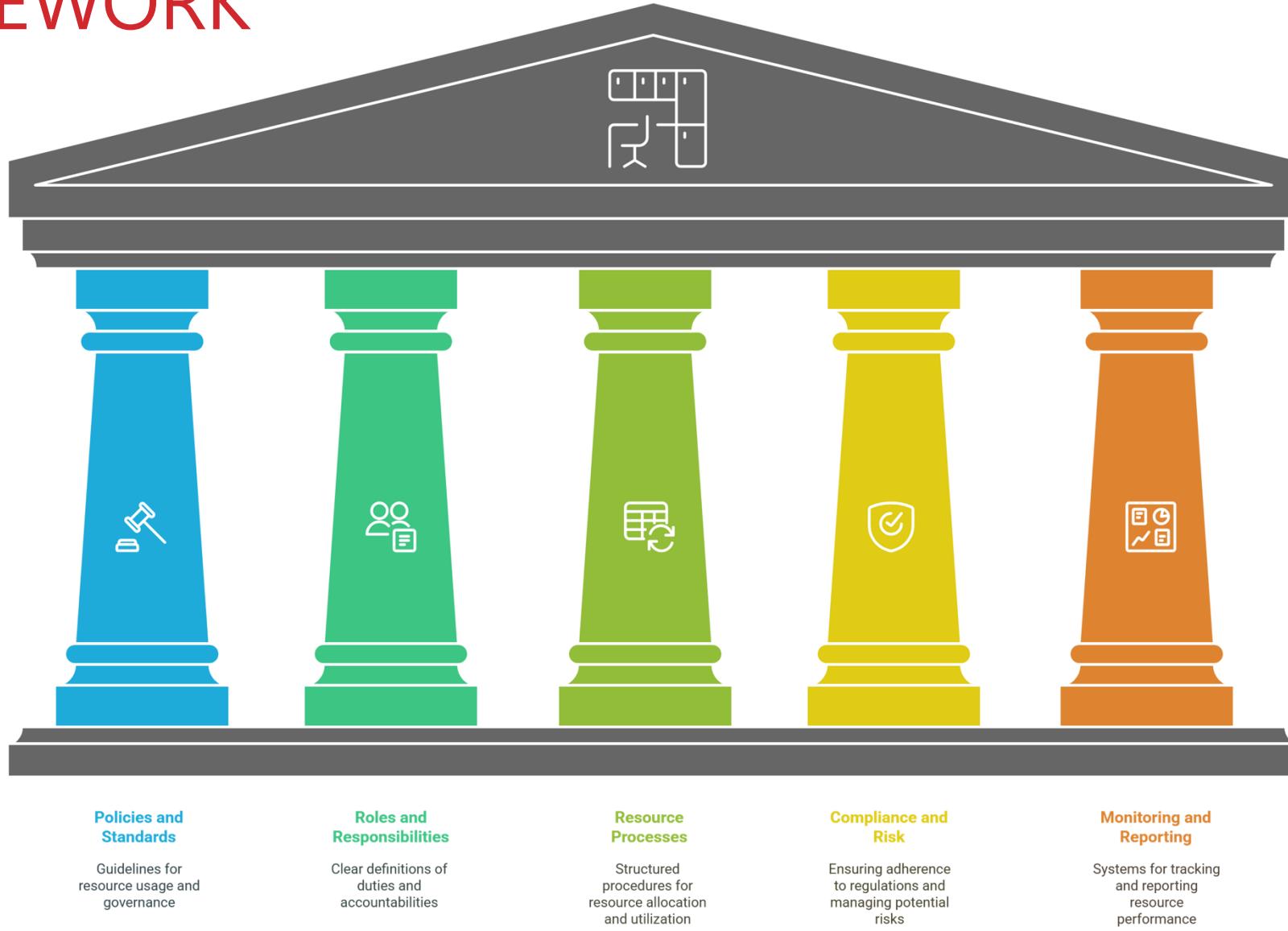
**Regular Audits:** Schedule periodic compliance checks

**Automate Monitoring:** Leverage tools for continuous oversight

**Training Programs:** Educate teams on governance protocols

**Documentation:** Keep detailed records of policies and changes

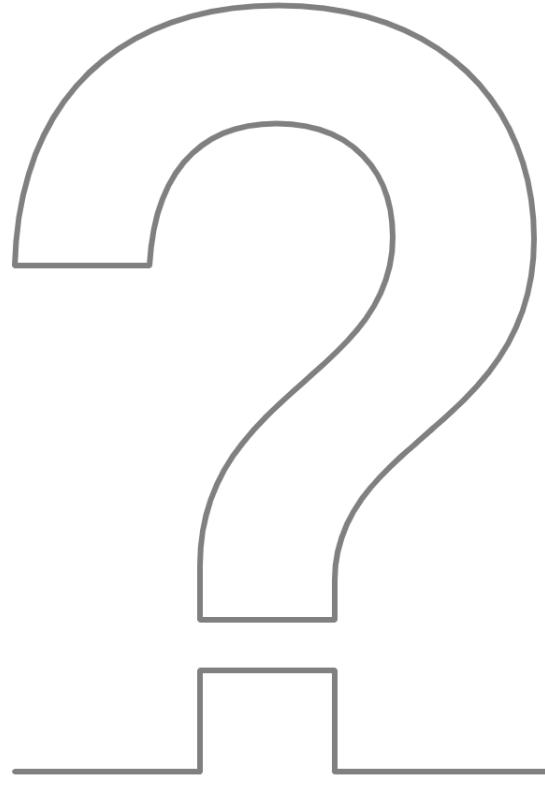
# KEY COMPONENTS OF A CLOUD GOVERNANCE FRAMEWORK



# BEST PRACTICES FOR CLOUD GOVERNANCE

- Align with IT policies
- Use COBIT, ITIL frameworks
- Segregate duties
- Regular training
- Continuous improvement

# CHOOSING THE RIGHT GOVERNANCE MODEL



## Centralized Model

Offers strong control and consistency but may lack agility.

## Decentralized Model

Enhances agility and innovation but may risk inconsistency.

## Federated Model

Balances control and agility by integrating elements of both models.

# DISCUSSION

Which governance model is best suited for a startup vs. an enterprise scenario?



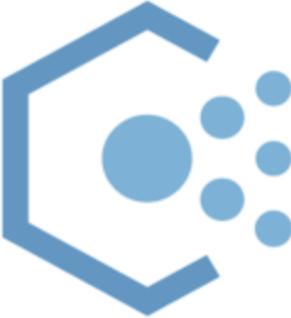
# IMPLEMENTING CLOUD GOVERNANCE

- Define objectives, select framework
- Use tools like Microsoft Purview
- Secure stakeholder buy-in
- Train staff, manage change
- Measure success via KPIs

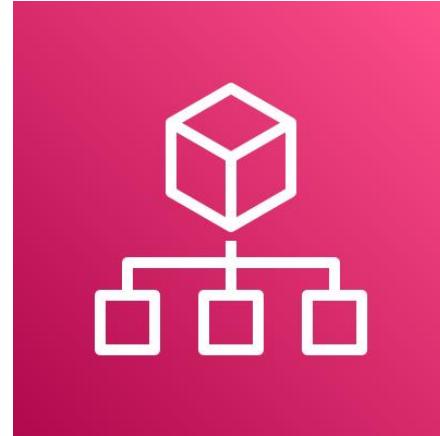
# TOOLS FOR CLOUD GOVERNANCE



Microsoft Purview



Azure Policy



**servicenow®**

# EXAMPLE

**Company:** Global manufacturer

**Challenge:** Multi-cloud management

**Solution:** COBIT framework

**Results:** Compliance, cost savings

**Lesson:** Stakeholder engagement

# ACTIVITY: ROLE-PLAY GOVERNANCE SCENARIO

## Description:

- Participants role-play stakeholders (e.g., CIO, security officer) resolving a governance issue (e.g., cost vs. security).

## Purpose:

- Understand governance challenges across roles.
- Practice decision-making.



# SECURITY STRATEGIES

- **Identity Management:** Use Microsoft Entra ID effectively
- **Encryption Standards:** Apply industry-leading encryption methods
- **Network Security:** Configure firewalls and VPNs properly
- **Real-Time Alerts:** Set up Azure Monitor for instant notifications
- **Regular Updates:** Continuously patch and update systems

# BUILDING A SECURITY CULTURE

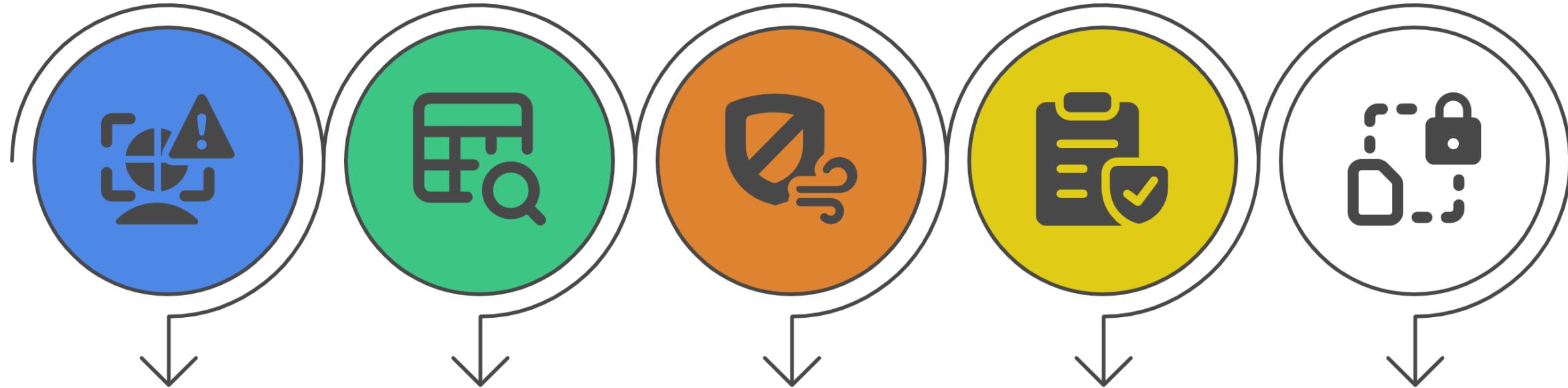


- **Training Programs:** Regular security training for all staff
- **Phishing Simulations:** Test and improve security awareness
- **Clear Communication:** Keep security policies transparent and accessible
- **Incentives:** Reward proactive security measures
- **Continuous Learning:** Update teams on emerging threats

# ENHANCING SECURITY AWARENESS

- **Regular Workshops:** Host sessions on the latest security threats
- **Interactive Training:** Use simulations and role-playing
- **Resource Libraries:** Maintain up-to-date security documentation
- **Feedback Channels:** Enable staff to report potential threats
- **Measurable Outcomes:** Track improvements in security posture

# CONTINUOUS MONITORING AND INCIDENT RESPONSE



## Monitoring Tools

Real-time security monitoring and alerting

## Log Management

Centralized logging and security analysis

## Incident Response

Plan for handling security incidents

## Security Audits

Regular security assessments and testing

## SIEM Integration

Security information and event management

# MEETING COMPLIANCE & REGULATORY REQUIREMENTS

- Regulations: GDPR, HIPAA, PCI DSS
- Provider certifications: SOC 2, ISO 27001
- Regular compliance audits
- Data sovereignty, jurisdiction
- Automated compliance checks

# INCIDENT RESPONSE & REMEDIATION



**Response Plan:** Develop a detailed incident response plan

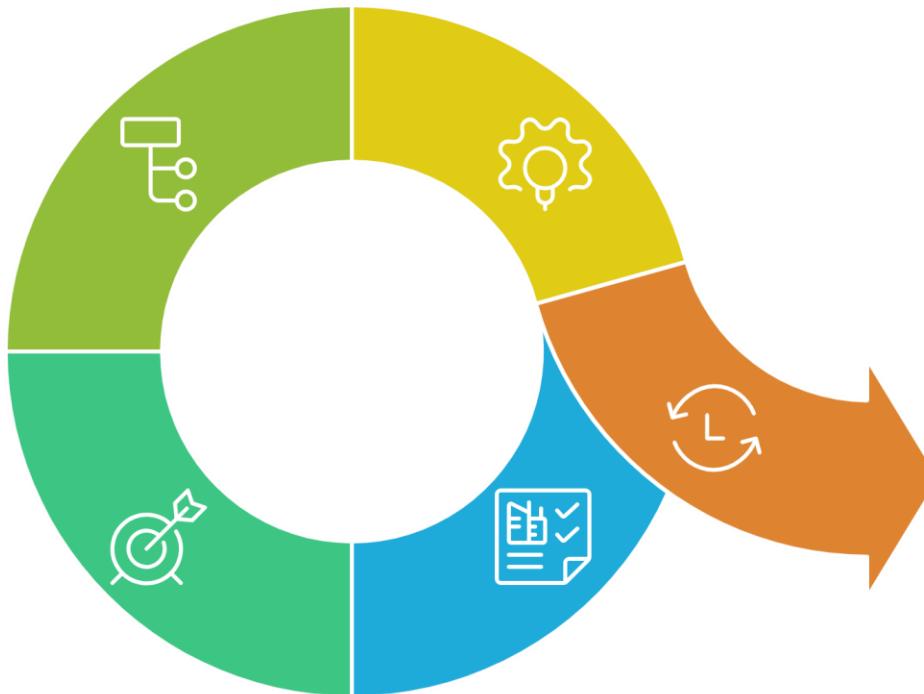
**Defined Roles:** Clearly assign responsibilities during a breach

**Communication Protocols:** Establish internal and external communication channels

**Post-Incident Reviews:** Analyze incidents for continuous improvement

**Azure Tools:** Utilize Azure Sentinel for threat detection and response

# DEVELOPING AN INCIDENT RESPONSE PLAN



1

## Plan Documentation

Clearly outline procedures and roles

2

## Simulation Drills

Regularly test the plan

3

## Communication Trees

Define escalation paths

4

## Lessons Learned

Incorporate feedback from incidents

5

## Continuous Updates

Keep the plan current

# WHY USE AZURE MONITOR AND LOG ANALYTICS?

**Centralized Monitoring:** Consolidate logs and performance data

**Real-Time Alerts:** Configure immediate notifications for anomalies

**Custom Dashboards:** Create visualizations tailored to your needs

**Data Correlation:** Analyze trends across multiple services

**Integration:** Seamlessly integrate with other Azure management tools

# FEATURES: AZURE MONITOR AND LOG ANALYTICS

The screenshot shows the Azure Monitor Overview page. On the left is a navigation sidebar with links for Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service health, Workbooks, Insights, Managed Services, Settings, and Support + Troubleshooting. The main content area has a banner about Log Analytics agents being deprecated. Below this, there's a section for 'Insights' with links to Application insights, Container Insights, and VM Insights. A 'Detection, triage, and diagnosis' section follows, featuring Metrics, Alerts, Logs, Diagnostic Settings, Azure Monitor SCOM managed instance, and Managed Prometheus.

**Dashboards:** Set up unified dashboards for key metrics

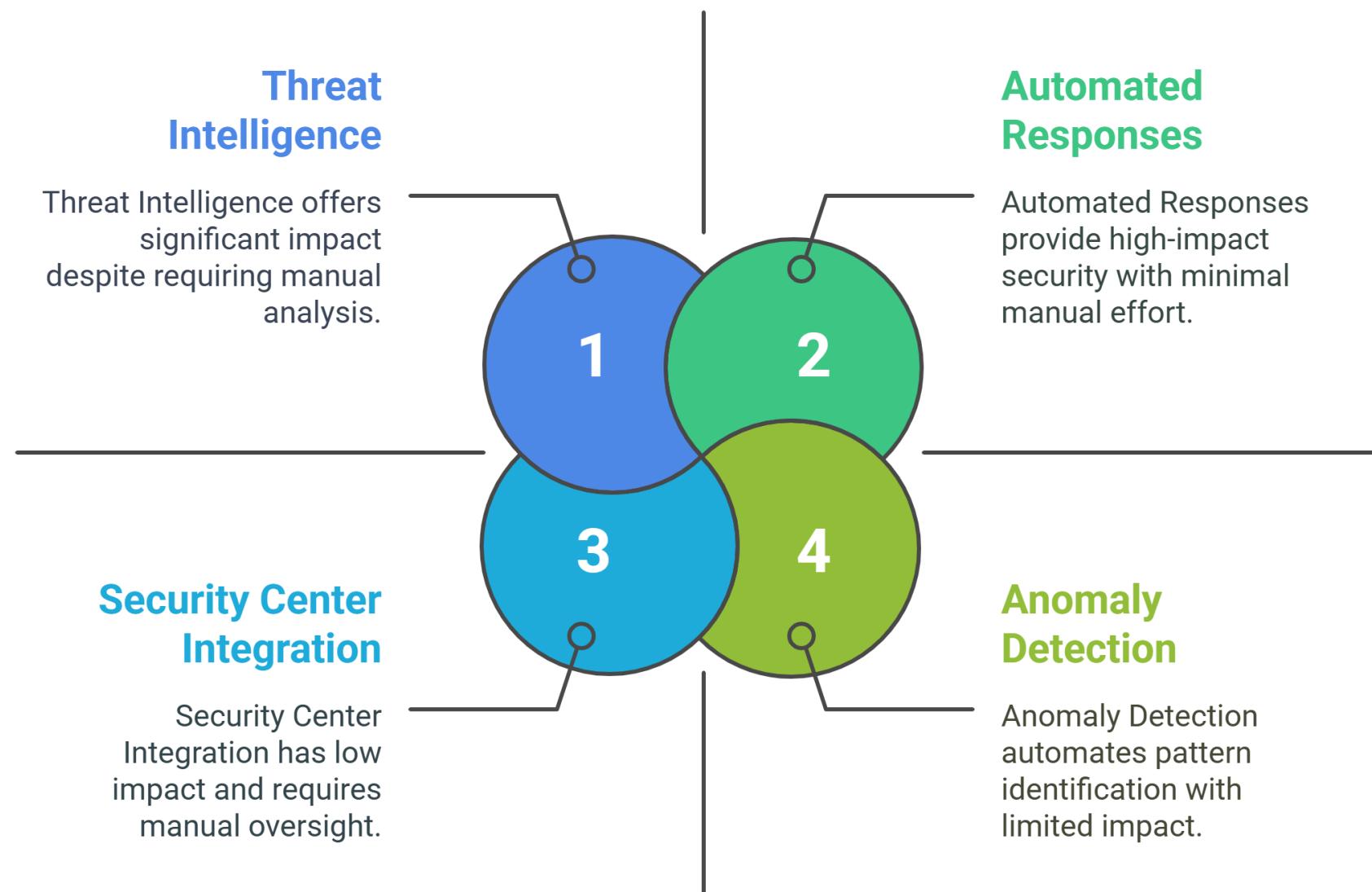
**Alert Rules:** Define thresholds to trigger alerts

**Log Querying:** Use Kusto Query Language (KQL) for detailed analysis

**Integration:** Connect with Azure Security Center for enhanced insights

**Regular Reviews:** Periodically refine your monitoring setup

# ADVANCED THREAT PROTECTION



# POP QUIZ:

You are tasked with ensuring that all resources in your Azure environment comply with your organization's governance standards. You need a solution that allows you to define and enforce policies across subscriptions and resources.

Which Azure service should you use?

- A. Azure Monitor
- B. Azure Sentinel
- C. Azure Policy**
- D. Azure Data Factory



# POP QUIZ:

You are tasked with ensuring that all resources in your Azure environment comply with your organization's governance standards. You need a solution that allows you to define and enforce policies across subscriptions and resources.

Which Azure service should you use?

- A. Azure Monitor
- B. Azure Sentinel
- C. Azure Policy**
- D. Azure Data Factory



# POP QUIZ:

You are securing sensitive information stored and transmitted within your Azure environment. To ensure data protection both at rest and in transit, you must apply a foundational security measure.

Which action should you take?

- A. Implement multi-factor authentication (MFA) for all users
- B. Configure virtual private networks (VPNs)
- C. Enable network firewalls
- D. Apply strong encryption techniques



# POP QUIZ:

You are securing sensitive information stored and transmitted within your Azure environment. To ensure data protection both at rest and in transit, you must apply a foundational security measure.

Which action should you take?

- A. Implement multi-factor authentication (MFA) for all users
- B. Configure virtual private networks (VPNs)
- C. Enable network firewalls
- D. Apply strong encryption techniques**



# ACTIVITY:

**Objective:** Assess personal understanding of cloud security

**Task:** Write down one security practice you think is most critical

**Discussion:** Share insights in small groups

**Outcome:** Identify common security themes

**Time:** 5 minutes



# INTRODUCTION TO CLOUD VENDOR MANAGEMENT

**Definition:** Managing cloud provider relationships

**Importance:** Mitigate dependency risks

**Lifecycle:** Selection, onboarding, management

**Challenges:** Lock-in, cost, security

**Leadership role:** Strategic oversight



VENDOR MANAGEMENT

# VENDOR SELECTION



- Evaluate vendors based on their reputation, reliability, and service offerings.
- Consider factors like security, compliance, and customer support.
- Look for providers that align with your organization's goals and values.
- Risk of choosing an unsuitable vendor leading to operational issues.
- Conduct thorough due diligence before selection.

# CONTRACT NEGOTIATION & MANAGEMENT

Negotiating cloud contracts is a complex process that requires balancing technical, legal, and business considerations to safeguard the organization's interests.

Effective contract management ensures that vendor relationships deliver value while minimizing risks.



## Data Control

Prioritize controlling your data instead of owning.



## Usable Format

Make sure data is returned in usable format.



## Security Measures

Negotiate strong security and privacy protections.



## Service Agreements

Define clear service level agreements.



## IP Ownership

Understand intellectual property ownership and licensing.



## Liability Limits

Address the limits of indemnity and liability.



## Cross-functional Teams

Involve teams from different departments.

# RISK ASSESSMENT OF VENDORS

- Conduct regular assessments (annually or bi-annually)
- Evaluate security controls and certifications
- Assess compliance with regulations
- Understand shared responsibility model
- Use CSPM tools for monitoring
- Prioritize risks by impact and likelihood
- Involve cross-functional teams

# SERVICE LEVEL AGREEMENTS



## Service Quality

Ensuring high standards and performance in service delivery



## Accountability

Establishing responsibility for service failures and outcomes



## Reliability

Guaranteeing consistent and dependable service availability



## Shared Responsibilities

Clarifying roles and duties among service stakeholders



## Communication

Fostering effective dialogue and interaction between parties

# ADDRESSING VENDOR LOCK-IN

- **Diversification:** Avoid dependence on a single provider
- **Interoperability:** Ensure systems work across platforms
- **Exit Strategies:** Develop clear migration plans
- **Contract Flexibility:** Negotiate favorable terms
- **Multi-Cloud Tools:** Use platforms to manage multiple clouds



# BEST PRACTICES

**Plan Ahead:** Develop a multi-cloud or hybrid strategy

**Evaluate Options:** Regularly review vendor roadmaps

**Contract Clauses:** Include exit and migration provisions

**Standardized APIs:** Use common interfaces for easier migration

**Azure Focus:** Leverage Azure Arc for multi-cloud management

# VENDOR OFFBOARDING

- Plan offboarding in advance
- Review termination clauses
- Ensure data return or deletion
- Revoke vendor access promptly
- Conduct compliance audits
- Document the process
- Communicate clearly
- Monitor post-offboarding risks



# ENSURING DATA PRIVACY & PROTECTION

**Sensitive Data:** Identify and classify critical data

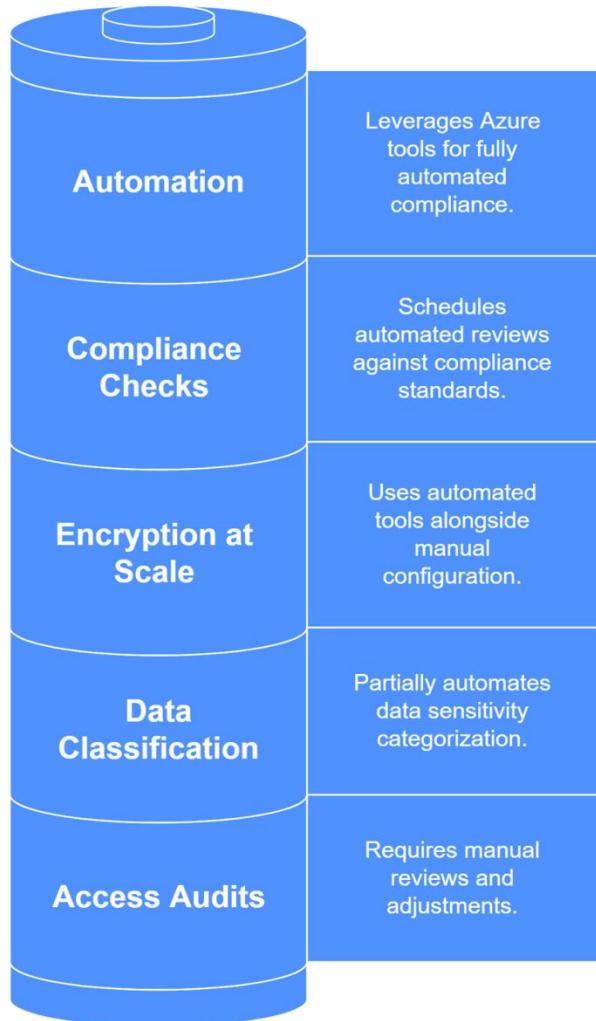
**Encryption Policies:** Enforce strong encryption practices

**Access Control:** Limit data access to authorized users

**Compliance:** Adhere to relevant privacy regulations

**Azure Tools:** Use Azure Key Vault for secure data management

# DATA PRIVACY STRATEGIES



**Data Classification:** Categorize data based on sensitivity

**Encryption at Scale:** Utilize both hardware and software encryption

**Access Audits:** Regularly review who has access to sensitive data

**Compliance Checks:** Schedule periodic reviews against standards

**Automation:** Use Azure tools for automated compliance reporting

# POP QUIZ:

You are reviewing security responsibilities under the Azure shared responsibility model. You need to determine which task falls under the customer's scope rather than Microsoft's.

Which responsibility is assigned to the customer?

- A. Ensuring physical security of Azure data centers
- B. Maintaining physical server hardware
- C. Securing and configuring application data
- D. Managing cooling and power infrastructure



# POP QUIZ:

You are reviewing security responsibilities under the Azure shared responsibility model. You need to determine which task falls under the customer's scope rather than Microsoft's.

Which responsibility is assigned to the customer?

- A. Ensuring physical security of Azure data centers
- B. Maintaining physical server hardware
- C. Securing and configuring application data**
- D. Managing cooling and power infrastructure



# RECAP: BUSINESS CONTINUITY & DISASTER RECOVERY



**DR Planning:** Develop comprehensive disaster recovery strategies

**Backup Solutions:** Implement regular, reliable backups

**Failover Mechanisms:** Ensure seamless transition during failures

**Testing:** Regularly simulate disaster scenarios

**Azure Services:** Utilize Azure Site Recovery and Backup

# RECAP: DISASTER RECOVERY PLANNING

**DR Documentation:** Maintain a clear, actionable DR plan

**Scheduled Drills:** Regularly test recovery procedures

**Data Redundancy:** Ensure backups are stored in multiple regions

**Recovery Objectives:** Define RTO (Recovery Time Objective) and RPO (Recovery Point Objective)

**Continuous Improvement:** Update DR plans based on drill outcomes

# REGULAR RISK ASSESSMENTS & AUDITS

**Scheduled Reviews:** Conduct periodic risk and compliance audits

**Assessment Tools:** Use automated tools for continuous evaluation

**Documentation:** Maintain records of audit findings and resolutions

**Stakeholder Involvement:** Involve key teams in the review process

**Action Plans:** Develop remediation strategies based on audit results



# CONDUCTING RISK ASSESSMENTS

**Comprehensive Checklists:** Use detailed checklists to cover all areas

**Automated Reporting:** Leverage tools like Azure Monitor for real-time data

**Periodic Reviews:** Schedule regular audits to capture evolving risks

**Feedback Loops:** Incorporate insights from assessments into improvements

**Benchmarking:** Compare findings against industry standards

# POP QUIZ:

## Question:

You are managing a cloud-based infrastructure for your organization. To maintain regulatory alignment and meet internal governance standards, you need to ensure continuous compliance.

Which approach should you implement?

- A. Perform a single compliance audit during initial deployment
- B. Trust that vendor certifications are sufficient for compliance
- C. Schedule and conduct recurring compliance audits
- D. Deprioritize policy updates unless mandated by an incident



# POP QUIZ:

## Question:

You are managing a cloud-based infrastructure for your organization. To maintain regulatory alignment and meet internal governance standards, you need to ensure continuous compliance.

Which approach should you implement?

- A. Perform a single compliance audit during initial deployment
- B. Trust that vendor certifications are sufficient for compliance
- C. Schedule and conduct recurring compliance audits**
- D. Deprioritize policy updates unless mandated by an incident



# POP QUIZ:

You are responsible for managing the performance and health of resources deployed in an Azure environment. You need a solution that allows you to collect, analyze, and act on telemetry data from multiple services.

Which Azure service should you use?

- A. Azure Data Factory
- B. Azure Virtual Network
- C. Azure Monitor
- D. Azure Cost Management



# POP QUIZ:

You are responsible for managing the performance and health of resources deployed in an Azure environment. You need a solution that allows you to collect, analyze, and act on telemetry data from multiple services.

Which Azure service should you use?

- A. Azure Data Factory
- B. Azure Virtual Network
- C. Azure Monitor**
- D. Azure Cost Management



# INDIVIDUAL KEY TAKEAWAYS



Write down three key insights from today's session.

Highlight how these take aways influence your work.

# COURSE REVIEW

Week 11 provided a comprehensive exploration into managing cloud risks, with a strong focus on the practical application of governance, security, and vendor management strategies in an Azure environment.

We discussed the importance of establishing robust governance frameworks, including the use of tools like Azure Policy and Blueprints to ensure compliance and continuous monitoring.

The session emphasized security best practices—from implementing strong access controls and data encryption to utilizing Azure Security Center and Sentinel for threat detection and incident response.

- Week 1-2: Introduction to Cloud Technology
- Week 3-5: Cloud Strategy and Architecture
- Week 6-7: Use Cases and Real-World Applications
- Week 8-9: Benefits and Value Proposition
- Week 10-12: Challenges and Risks
- Week 13-14: Interactive Simulations and Practical Exercises
- Week 15: Course Review and Final Assessment

# NEXT WEEK: SCENARIO-BASED DISCUSSIONS

**Interactive Group Activities:** Engage in scenario-based exercises to apply risk mitigation strategies.

**Real-World Case Studies:** Analyze detailed cloud risk incidents and develop actionable response plans.

**Collaborative Problem Solving:** Work in teams to identify challenges and propose innovative solutions.

**Focus on Practical Application:** Utilize Azure tools and best practices to address real-world issues.

**Outcome-Oriented Discussions:** Prepare to share insights and refine strategies for improved cloud resilience.

# Q&A AND OPEN DISCUSSION



