WEEK 12: SCENARIO-BASED DISCUSSIONS

TEKsystems Global Services

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 11

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

- 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

AGENDA

- **Overview of Activities:** Brief rundown of all scenarios

- **Group Formation:** Instructions for team creation and role assignments

- **Scenario Walkthroughs:** Step-by-step instructions for each scenario

- **Presentation Preparation:** Guidelines for presenting your findings

- **Q&A and Feedback:** Final discussion and reflection session

OVERVIEW OF INTERACTIVE ACTIVITY

Purpose: Apply risk management in practical scenarios

Format: Scenario-based group discussions

Tools Provided: Risk assessment templates, scenario briefs, SWOT templates

Time Allocation: Approximately 60 minutes of group work

Expected Outcome: Develop and present integrated risk mitigation plans

FORM GROUPS

Form Groups: Create teams of 4–6 participants

Assign Roles: Facilitator, Note-taker, Presenter, Analyst, Timekeeper

Define Responsibilities: Clearly outline each role's duties

Balance Participation: Ensure every member contributes

Record Roles: Write down each member's role on a provided worksheet

SCENARIO 1: COST OVERRUN

SCENARIO 1

Scenario Summary: Company Alpha's Azure migration has blown past budget by 30%. Beyond egress fees and basic delays, deeper issues emerged:

Hidden Licensing Charges:
Third-party software licenses (e.g., SQL Server, monitoring tools) were not converted to Azure Hybrid Benefit, adding unexpected costs of $25K.

Data Processing Costs:
High-frequency ETL jobs in Azure Data Factory incurred premium "data movement" charges of $15K.

Network Topology Inefficiencies:
Cross-region traffic between VNets added network peering fees of $10K.

Integration Delays:
Custom API connectors took 3 extra weeks to stabilize, leading to $30K in consulting overrun.

Resource Misallocation:
40% of VMs were left running at "Standard_D4s_v3" during off-hours rather than scaled down, costing an extra $20K.

25000 Hidden Licenses
30000 Integration delays
25000 Data Processing Costs
40000 Resource Misallocation
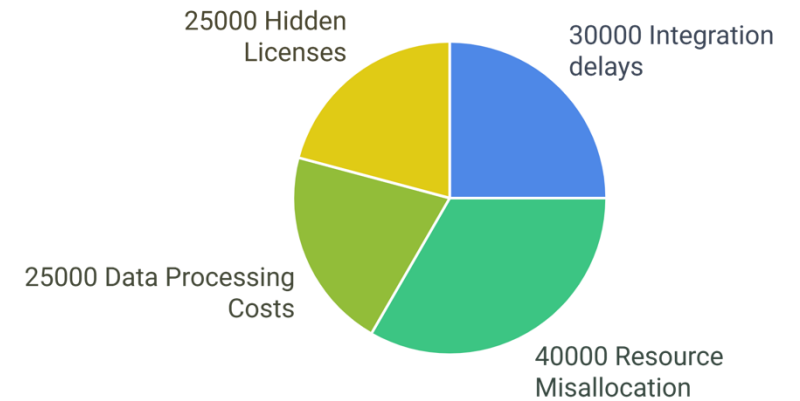
INSTRUCTIONS FOR SCENARIO 1

Step 1: Read the scenario brief provided on the next slide

Step 2: Identify at least three key factors contributing to the cost overruns

Step 3: Brainstorm potential mitigation strategies within your group

Step 4: Complete the risk assessment template with your analysis and proposed solutions

Step 5: Prepare a 5-minute presentation summarizing your group's findings

GROUP DISCUSSION: SCENARIO 1

Open Dialogue: Every member must share insights

Use the Whiteboard: Document ideas and key points on a shared digital whiteboard or flipchart

Focus on Root Causes: Identify primary factors behind the cost overruns

Develop Solutions: Brainstorm actionable mitigation strategies

Document Findings: Record your discussion on the risk assessment template

9

SCENARIO 2: SECURITY BREACH

10

SCENARIO 2: SECURITY BREACH

Scenario Focus: Addressing a security breach incident in Azure

Key Challenges: Misconfigured access controls, inadequate monitoring, and delayed incident response

Task Objective: Analyze the breach and propose an improved security plan

Deliverable: A detailed incident response improvement plan

Tools Provided: Security improvement template

SCENARIO 2: INSTRUCTIONS

Step 1: Read the security breach scenario carefully on this slide

Step 2: Identify at least three misconfigurations or security gaps

Step 3: Brainstorm improvements for the incident response plan

Step 4: Document your analysis in the security improvement template

Step 5: Prepare a concise summary for your group presentation

BRIEF: SECURITY BREACH

Scenario Summary: Company Beta experienced a security breach after unauthorized access was detected.

Key Data Points:
- Access controls were misconfigured, allowing external access.
- Incident logs show delayed response times and lack of automated alerts.
- The breach resulted in data exposure and temporary service downtime.

Impact: Led to customer trust issues and significant operational disruption.
Additional Note: Focus on the need for proactive monitoring and robust access control.

GROUP DISCUSSION

Analyze the Timeline: Review the breach timeline and incident logs together

Identify Gaps: Pinpoint misconfigurations and response failures

Propose Solutions: Brainstorm enhancements for incident response protocols

Document Changes: Record proposed improvements in the security template

Prepare Summary: Outline your revised security plan for presentation

SCENARIO 3: VENDOR LOCK-IN
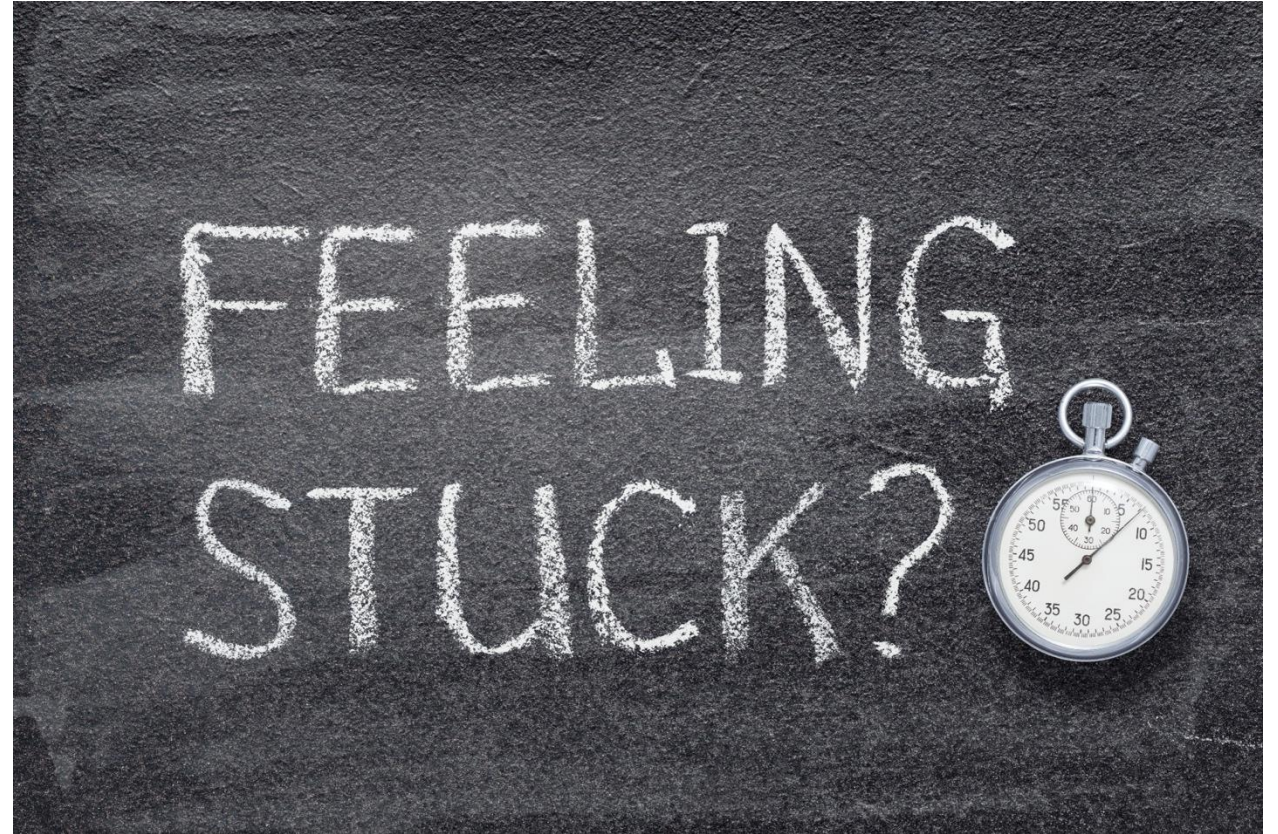
SCENARIO 3: VENDOR LOCK-IN

Scenario Focus: Overcoming over-dependence on a single cloud vendor

Key Challenges: Contractual rigidity, high switching costs, and limited innovation

Task Objective: Develop a multi-cloud diversification strategy

Deliverable: A SWOT analysis and an actionable vendor diversification plan

Tools Provided: SWOT analysis template

SCENARIO 3: INSTRUCTIONS

Step 1: Read the vendor lock-in scenario details on the next slide

Step 2: Identify the risks and challenges related to vendor dependency

Step 3: Conduct a SWOT analysis to evaluate the current vendor reliance

Step 4: Develop actionable steps to diversify your vendor relationships

Step 5: Document your SWOT analysis and prepare a presentation summary

SCENARIO 3: BRIEF

Scenario Summary: Company Gamma is heavily reliant on a single cloud vendor, restricting innovation.

Key Data Points:
- Contractual limitations prevent switching vendors.
- High switching costs and limited scalability were noted.
- The company's innovation and flexibility are stifled due to vendor dependency.

Impact: Reduced agility and inability to leverage new technologies.
Additional Note: Focus on creating strategies for vendor diversification.

SCENARIO 3: GROUP DISCUSSIONS

Evaluate Dependency: Discuss how vendor lock-in affects flexibility

Conduct SWOT Analysis: Complete the SWOT template collaboratively

Identify Strategies: Brainstorm actionable steps for vendor diversification

Record Findings: Document all insights and proposed solutions

Prepare Presentation: Summarize your SWOT analysis and diversification plan

19

SCENARIO 4: INTEGRATION BOTTLENETCKS

SCENARIO 4: OVERCOMING INTEGRATION BOTTLENECKS

Evaluate Dependency: Discuss how vendor lock-in affects flexibility

Conduct SWOT Analysis: Complete the SWOT template collaboratively

Identify Strategies: Brainstorm actionable steps for vendor diversification

Record Findings: Document all insights and proposed solutions

Prepare Presentation: Summarize your SWOT analysis and diversification plan

21

SCENARIO 4: INSTRUCTIONS

Step 1: Read the integration bottleneck scenario details on this slide

Step 2: Identify at least three major integration issues

Step 3: Brainstorm automation and process optimization strategies

Step 4: Document your proposed improvements in the integration template

Step 5: Prepare a brief presentation outlining your action plan

SCENARIO 4: BRIEF

Scenario Summary: Company Delta is experiencing significant performance lags due to integration failures.

Key Data Points:
Error logs indicate frequent data flow interruptions.
System performance reports show delayed processing times.
Inconsistent integration between legacy and cloud applications.

Impact: Reduced operational efficiency and delayed service delivery.
Additional Note: Focus on streamlining processes and implementing automation solutions.

SCENARIO 4: GUIDELINES FOR DISCUSSION

Identify Bottlenecks: List key integration issues impacting performance

Brainstorm Solutions: Develop automation and optimization strategies

Document Strategies: Record your proposals in the integration improvement template

Ensure Actionability: Focus on solutions that are practical and measurable

Prepare to Present: Summarize your action plan for class discussion

SCENARIO 5: COMPLIANCE SETBACKS

SCENARIO 5: MANAGING COMPLIANCE SETBACKS

Scenario Focus: Addressing challenges in meeting regulatory requirements

Key Challenges: Compliance gaps, audit failures, and inadequate documentation

Task Objective: Develop a compliance improvement roadmap

Deliverable: A detailed roadmap outlining specific remediation steps

Tools Provided: Compliance roadmap template

SCENARIO 5: INSTRUCTIONS

Step 1: Read the compliance setback scenario details on this slide

Step 2: Identify at least three compliance gaps from the scenario

Step 3: Brainstorm actionable remediation steps for each gap

Step 4: Document your compliance roadmap using the provided template

Step 5: Prepare a concise summary of your roadmap for presentation

SCENARIO 5: BRIEF

Scenario Summary: Company Epsilon is facing significant compliance challenges and has failed recent audits.

Key Data Points:
Audit reports reveal multiple instances of non-compliance.
Documentation gaps have led to regulatory penalties.
There is a lack of systematic compliance checks.

Impact: Risk of fines, operational delays, and reputational damage.
Additional Note: Emphasize actionable steps to close the gaps and improve compliance.

SCENARIO 5: DISCUSSION GUIDELINES

Review Data: Analyze the provided audit reports and compliance charts together

Identify Key Issues: List the major compliance gaps in the scenario

Develop Remediation Steps: Brainstorm and document actionable solutions

Complete the Template: Use the compliance roadmap template to record your plan

Prepare to Present: Summarize your roadmap and be ready to share with the class

SCENARIO 6: PERFORMANCE OPTIMIZATION

SCENARIO 6: OPTIMIZING PERFORMANCE

Scenario Focus: Addressing performance issues across multiple cloud platforms

Key Challenges: Latency, resource allocation inefficiencies, and data synchronization problems

Task Objective: Develop a multi-cloud performance optimization plan

Deliverable: A detailed plan with defined performance metrics

Tools Provided: Performance optimization template

31

SCENARIO 6: INSTRUCTIONS

Step 1: Read the multi-cloud performance scenario details on this slide

Step 2: Identify key performance bottlenecks affecting operations

Step 3: Brainstorm strategies to improve resource allocation and data synchronization

Step 4: Document your proposed plan in the performance optimization template

Step 5: Prepare to present your plan, including specific performance metrics

SCENARIO 6: BRIEFING

Scenario Summary: Company Zeta is experiencing significant latency and resource issues in a multi-cloud setup.

Key Data Points:

- Performance logs indicate high latency during peak hours.
- Customer feedback highlights slow response times.
- Resource usage reports show imbalances across cloud platforms.

Impact: Decreased efficiency and reduced customer satisfaction.

Additional Note: Focus on strategies that streamline resource allocation and improve data synchronization.

SCENARIO 6: GUIDELINES

Identify Bottlenecks: Discuss and list the performance issues identified in the scenario

Brainstorm Solutions: Develop strategies to optimize resource allocation and data synchronization

Define Metrics: Identify specific performance metrics to track improvements

Document Findings: Record your solutions in the performance optimization template

Prepare to Present: Summarize your optimization plan for class discussion

SCENARIO 7: DEALING WITH CHAOS

SCENARIO 7: MULTIPLE CHALLENGES

Scenario Focus: Addressing multiple challenges simultaneously (cost, security, vendor, and performance)

Key Challenge: Develop a holistic risk mitigation plan that integrates all risk areas

Task Objective: Synthesize learnings from previous scenarios into one comprehensive plan

Deliverable: A unified action plan and a 10-minute group presentation

Tools Provided: Unified action plan template and integrated scenario brief

SCENARIO 7: INSTRUCTIONS

Step 1: Read the integrated scenario brief on this slide

Step 2: Identify key risks in each category (cost, security, vendor, performance)

Step 3: Discuss and compile a list of combined mitigation strategies

Step 4: Document your integrated plan in the unified action plan template

Step 5: Prepare a 10-minute presentation summarizing your plan

SCENARIO 7: BRIEFING

Scenario Summary: Company U is facing simultaneous challenges across cost, security, vendor, and performance areas.

Key Data Points:
- Financial reports indicate a 25% budget overrun.
- Security logs reveal multiple misconfigurations leading to breaches.
- Vendor contracts are rigid, limiting flexibility.
- Performance metrics show high latency and resource imbalances.

Impact: Severe operational disruption and significant financial losses.
Additional Note: Your plan should integrate strategies to address all these risk areas holistically.

SCENARIO 7: GUIDELINES

Collaborate Closely: Ensure every member contributes to the integrated plan

Identify Interdependencies: Discuss how different risk areas affect one another

Develop Comprehensive Strategies: Combine mitigation approaches from previous scenarios

Document Thoroughly: Use the unified action plan template to record your integrated plan

Prepare Presentation: Summarize your key findings and prepare for a detailed 10-minute presentation

CHECK IN – GROUP PROGRESS REPORT

Instruction: Each group presents a 2-minute update on your progress so far '

Key Points: Share major challenges encountered and preliminary solutions

Feedback: Facilitators will provide real-time input

Documentation: Record progress and roadblocks on your templates

Outcome: Ensure groups are on track for a comprehensive plan

PREPARE FOR PRESENTATIONS

Task: Consolidate your integrated risk mitigation plan

Role Assignment: Confirm your group's designated presenter(s)

Rehearse: Practice summarizing the key points of your plan

Document Check: Ensure all templates and documentation are complete

Visual Aids: Prepare additional charts or diagrams to support your presentation

PRESENTATIONS - INSTRUCTIONS

Presentation Time: Each group has 10 minutes to present their integrated plan

Content Requirements: Cover risk identification, mitigation strategies, and expected outcomes

Template Usage: Base your presentation on your unified action plan template

Q&A Session: Allow 2–3 minutes for questions after each presentation

Evaluation Criteria: Clarity, feasibility, integration, and innovation of your plan

PRESENTATION FEEDBACK

Feedback Focus: Clarity, feasibility, and integration of strategies

Peer Input: Engage in constructive critique after each presentation

Facilitator Guidance: Facilitators will provide targeted recommendations

Documentation: Record key feedback for future improvements

Outcome: Use feedback to refine your integrated plan further

REFLECTION

Task: Individually write down one key insight from today's session
Focus: Reflect on how integrated risk management can be applied in your role
Discussion: Share your insight with a partner or small group
Documentation: Record your reflection in your personal action plan worksheet
Outcome: Strengthen your personal commitment to continuous improvement

COURSE REVIEW

Week 11 marked a pivotal shift from theory to practice as you engaged in scenario-based group discussions designed to test and apply your understanding of cloud risk management.

This hands-on approach emphasized critical thinking, collaboration, and structured problem-solving under real-world-inspired constraints.

- 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: SIMULATIONS

Next week, we shift from the whiteboard to the Azure Portal with guided hands-on labs. You'll deploy core Azure services like virtual machines and web apps—not just to click buttons, but to understand the architecture and rationale behind each configuration. We'll walk through virtual networking and storage account setups, focusing on best practices for both security and performance.

Then we'll introduce Azure Monitor and related tools to help you track costs, usage, and performance in real time. For governance, we'll touch on resource policies—how organizations can enforce rules at scale.

Q&A AND OPEN DISCUSSION

THANK YOU