CC9 - Risk Mitigation

# Prompt 1

CC9.1: The entity develops risk mitigation activities for potential business disruptions.

Document: BCDR, Section: Contingency Planning and FISCAM

CC9.1.1: Documented policies and procedures effectively guide personnel in developing control activities to mitigate risks, as confirmed by an inspection with no exceptions noted.

Document: BCDR, Section: Contingency Planning and FISCAM

CC9.1.2: Annual risk assessments identify threats to in-scope systems, with checkpoints ensuring critical teams join the Service Resiliency Program, confirmed by an inspection with no exceptions noted.

Document: BCDR, Section: Business Impact Analysis (BIA)

CC9.1.3: High or critical risks related to services or data centers are reviewed, assigned an owner, and remediated per the Cloud Vendor risk management program, confirmed by an inspection with no exceptions noted.

Document: BCDR, Section: BIA and BCP Metrics

CC9.1.4: Cloud Vendor maintains and annually reviews a Business Impact Analysis (BIA) and Service Resiliency Plan (SRP) for each service, outlining disaster procedures, ownership, roles, and responsibilities, confirmed by an inspection with no exceptions noted.

Document: BCDR, Section: Business Impact Analysis (BIA)

CC9.2: Vendor and business partner risk management.

Document: Trust-services-criteria, Section: Risk Mitigation

CC9.2.1: The Supplier Code of Ethics and Business Conduct, along with the Supplier and Physical Security Standards, outline the requirements for suppliers and vendors, confirmed by an inspection with no exceptions noted.

Document: Trust-services-criteria, Section: Risk Mitigation

CC9.2.2: Cloud Vendor annually reviews data center provider attestation reports or certifications, evaluates and tracks issues, and assesses sites without reports or certifications, confirmed by an inspection with no exceptions noted.

Document: SOC Auditing, Section: Sub-Service Organizations

CC9.2.3: Cloud Vendor performs annual risk assessments to identify threats to in-scope systems, with checkpoints ensuring critical teams join the Service Resiliency Program, confirmed by an inspection with no exceptions noted.

Document: BCDR, Section: Business Impact Analysis (BIA)

CC9.2.4: High or critical risks related to services or data centers are reviewed, assigned an owner, and remediated according to the Cloud Vendor risk management program, confirmed by an inspection with no exceptions noted.

Document: BCDR, Section: BIA and BCP Metrics

# Prompt 2

CC3.2.2: Periodic risk reviews are important as technology and threats change. Inherent risk is the chance of a misstatement due to error or fraud before controls are applied. Regular reviews help update risk assessments to reflect new threats and changes in technology. The SOC report shows how organizations update their risk assessments to manage these evolving risks.

CC3.4.1: Implementing controls helps reduce risks. Control risk values are checked by testing samples of transactions. The SOC report shows how controls, like having different people enter and approve transactions, are tested to ensure they work. This demonstrates the practical application of course concepts in verifying control effectiveness.

CC3.4.2: Monitoring and managing residual risks is key. Control risk estimates are verified through sampling and judgment. The SOC report shows how organizations keep an eye on residual risks and adjust their assessments to stay within acceptable limits. This aligns with the course's emphasis on continuous risk assessment and management.