Domain: Guardrails (GCP Detective and Auto-responsive Controls)

e.g. Public Cloud Accounts: GCP Onboarding

Objective	As a Cloud SOC Team, I need the Continuous Production Testing Framework for Guardrails ("Superposition") for behavioural end-to-end testing of guardrails in Citi.com.
Acceptance Criteria	• Deployment and Production Enablement: The Superposition Framework must be fully deployed and operational in the production environment (citi.com) for GCP. • Access Control: Access to Superposition must be strictly controlled, following the principle of least privilege, and should be limited to authorized Cloud Security team members. • Validation and Operationalization: The framework should be validated by the SOC team to ensure it effectively tests the efficacy of detective and auto-responsive security controls in production. • Infrastructure Management: All infrastructure supporting the superposition framework must be managed through LSE+TFE based pipelines to ensure consistent and automated deployments. • Automated behavioural testing environment: A dedicated security testing environment must be available for continuous behavioural testing of the guardrails' functionality and efficacy.
Stakeholders	• Cloud Security Controls Engineering Team [Chris Coleman]: Responsible for developing and deploying Superposition. • Cloud SOC Team [Bill Clements]: Primary customers of Superposition. • SDLC Platform Team: Ensures infra components can be deployed with TFE+Lightspeed pipelines. • CISO Manifold for certification of Superposition
Resourcing	• CISO Manifold for Superposition ISRP certification (including Threat Modelling)
Milestones	Describe what can be reasonably delivered by March and any future milestones • RFP approved • Manifold/ISRP AL 5 for Solution • Security testing folder deployed in citi.com [IAM Team]: `fldr-securitytesting` must be deployed in citi.com organization to have a safe environment to test security controls. • Superposition execution project created [Accounts]: The superposition execution folder `prj-cm-superposition` should be created under the security testing folder `fldr-securitytesting` • Superposition bad actor folder created [IAM]: The superposition bad actor folder `fldr-sp-testing` should be created under the security testing folder `fldr-securitytesting`. • Superposition bad actor project created [Accounts]: The superposition bad actor project `prj-sp-innerloop` should be created under the superposition bad actor folder `fldr-sp-testing`. • Superposition execution deployed to project [SecEng/Chris Coleman]: Superposition execution project should be deployed to `prj-cm-superposition` via LSE+TFE pipelines. • Superposition able to clean lingering resources [SecEng/Chris Coleman]: The bad actor `prj-sp-innerloop` should be able to be kept pristine before we use it for regular testing. • Superposition able to test in bad actor project [SecEng/Chris Coleman]: The superposition execution project `prj-cm-superposition` should be able to run tests in the bad actor account `prj-sp-innerloop`.
Submitter	Michael Lysaght/Christoper Coleman

Please reach out to Haripriya Jagannathan/Siddhi Revandkar/Dolapo Kukoyi once the document is ready for review and post it in **GCP Public Cloud Enablement-CTI-NAM** >> **Foundations** channel >> **User Stories** File by Oct 3rd

For Reviewers Use Only

Feedback	Feedback will be provided by reviewers here. Reviewers should record feedback as follow. Date – Reviewer Name – Feedback e.g. 2 Oct, 2024 – Mo Alslaoom – consider deletion of requested accounts to be added to success criteria.
Status	Review | Approved

Domain: User Story Title

Objective	
Acceptance Criteria	
Stakeholders	
Resourcing	
Milestones	
Submitter	

For Reviewers Use Only

Feedback	
Status	